

July 2011

INFORMATION
SHARING
ENVIRONMENT

Better Road Map
Needed to Guide
Implementation and
Investments

U.S. Government Accountability Office

GAO90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

Why GAO Did This Study

Recent planned and attempted acts of terrorism on U.S. soil underscore the importance of the government's continued need to ensure that terrorism-related information is shared in an effective and timely manner. The Intelligence Reform and Terrorism Prevention Act of 2004, as amended, mandated the creation of the Information Sharing Environment (ISE), which is described as an approach for sharing terrorism-related information that may include any method determined necessary and appropriate. GAO was asked to assess to what extent the Program Manager for the ISE and agencies have (1) made progress in developing and implementing the ISE and (2) defined an enterprise architecture (EA) to support ISE implementation efforts. In general, an EA provides a modernization blueprint to guide an entity's transition to its future operational and technological environment. To do this work, GAO (1) reviewed key statutes, policies, and guidance; ISE annual reports; and EA and other best practices and (2) interviewed relevant agency officials.

What GAO Recommends

GAO recommends that in defining a road map for the ISE, the Program Manager ensure that relevant initiatives are leveraged, incremental costs are defined, and an EA program management plan is established that defines how EA management practices and content will be addressed. The Program Manager generally agreed with these recommendations.

View [GAO-11-455](#) or key components. For more information, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov or David Powner at (202) 512-9286 or pownerd@gao.gov.

INFORMATION SHARING ENVIRONMENT

Better Road Map Needed to Guide Implementation and Investments

What GAO Found

Since GAO last reported on the ISE in June 2008, the Program Manager for the ISE and agencies have made progress in implementing a discrete set of goals and activities and are working to establish an "end state vision" that could help better define what the ISE is intended to achieve and include. However, these actions have not yet resulted in a fully functioning ISE. Consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act), the ISE is to provide the means for sharing terrorism-related information across five communities—homeland security, law enforcement, defense, foreign affairs, and intelligence—in a manner that, among other things, leverages ongoing efforts. To date, the ISE has primarily focused on the homeland security and law enforcement communities and related sharing between the federal government and state and local partners, to align with priorities the White House established for the ISE. It will be important that all relevant agency initiatives—such as those involving the foreign affairs and intelligence communities—are leveraged by the ISE to enhance information sharing governmentwide. The Program Manager and agencies also have not yet identified the incremental costs necessary to implement the ISE—which would allow decision makers to plan for and prioritize future investments—or addressed GAO's 2008 recommendation to develop procedures for determining what work remains. Completing these activities would help to provide a road map for the ISE moving forward. The administration has taken steps to strengthen the ISE governance structure, but it is too early to gauge the structure's effectiveness.

The Program Manager and ISE agencies have developed architecture guidance and products to support ISE implementation, such as the *ISE Enterprise Architecture Framework*, which is intended to enable long-term business and technology standardization and information systems planning, investing, and integration. However, the architecture guidance and products do not fully describe the current and future information sharing environment or include a plan for transitioning to the future ISE. For example, the EA framework describes information flows for only 3 of the 24 current business processes. In addition, the Program Manager's approach to managing its ISE EA program does not fully satisfy the core elements described in EA management best practices. For example, an EA program management plan for the ISE does not exist. The Program Manager stated that his office's approach to developing ISE architecture guidance is based on, among other things, the office's interpretation of the Intelligence Reform Act. Nevertheless, the act calls for the Program Manager to, among other things, plan for and oversee the implementation of the ISE, and officials from the key agencies said that the lack of detailed and implementable ISE guidance was one limiting factor in developing agency information sharing architectures. Without establishing an improved EA management foundation, including an ISE EA program management plan, the federal government risks limiting the ability of ISE agencies to effectively plan for and implement the ISE and more effectively share critical terrorism-related information.

Contents

Letter		1
	Background	6
	Program Manager and Agencies Have Advanced Key Information Sharing Activities but Have Not Yet Developed a Comprehensive Road Map to Effectively Implement the ISE	11
	The Enterprise Architecture Management Foundation for Supporting ISE Implementation Could Be Improved	28
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments and Our Evaluation	37
Appendix I	Objectives, Scope, and Methodology	43
Appendix II	ISE Framework Goals and Subgoal Activities	48
Appendix III	Analysis of ISE Architecture Content	50
Appendix IV	ISE's Satisfaction of Selected EA Institutional Leadership and Management Controls	53
Appendix V	Analysis of Information Sharing Segment Architectures	61
Appendix VI	Comments from the Program Manager for the Information Sharing Environment	69
Appendix VII	Comments from the Department of Homeland Security	74
Appendix VIII	GAO Contacts and Staff Acknowledgments	75

Tables

Table 1: ISE Architecture's Satisfaction of Relevant EA Guidance	50
Table 2: ISE's Satisfaction of Selected EAMMF Core Elements	53
Table 3: DOD Satisfaction of Information Sharing Segment Architecture Development Steps	61
Table 4: DHS Satisfaction of Information Sharing Segment Architecture Development Steps	63
Table 5: DOJ Satisfaction of Information Sharing Segment Architecture Development Steps	66

Abbreviations

AWN	Alerts, Warnings, and Notifications
CAR	Chief Architects Roundtable
CIO	Chief Information Officer
CISS	Common Information Sharing Standards
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
EA	enterprise architecture
EAF	Enterprise Architecture Framework
EAMMF	Enterprise Architecture Management Maturity Framework
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISSA	Information Sharing Segment Architecture
IT	information technology
JISSA	Justice Information Services Segment Architecture
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PAIS	Profile and Architecture Implementation Strategy
SAR	Suspicious Activity Reporting
SIPRNet	Secret Internet Protocol Router Network

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



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 21, 2011

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

The Honorable Ileana Ros-Lehtinen
Chairman
The Honorable Howard L. Berman
Ranking Member
Committee on Foreign Affairs
House of Representatives

Recent planned and attempted acts of terrorism on U.S. soil underscore the importance of the federal government's continued need to ensure that terrorism-related information is shared with stakeholders across all levels of government, the private sector, and foreign countries in an effective and timely manner.¹ To facilitate this sharing, section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), required the President to create an Information Sharing Environment (ISE)—an approach to facilitate the sharing of terrorism and homeland security information, which may include any methods determined necessary and appropriate.² In accordance with the act, the President designated a

¹ For purposes of this report, "terrorism-related information" encompasses "terrorism information," "homeland security information," and "weapons of mass destruction information," as defined by the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, as well as law enforcement information relating to terrorism or the security of the homeland. See Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70 (2004) (codified as amended at 6 U.S.C. § 485). See also Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan* (November 2006) at xxii (describing other categories of information recommended for inclusion in the ISE).

² See Pub. L. No. 108-458, § 1016 Stat. at 3664-70 (codified as amended by Pub. L. No. 110-53, § 504, 121 Stat. 266, 313-17 (2007), and Pub. L. No. 111-259, § 806(a)(1), 124 Stat. 2654, 2748 (2010) at 6 U.S.C. § 485). See also Pub. L. No. 107-296, § 892, 116 Stat. 2135, 2253-55 (2002) (requiring the establishment of procedures for the sharing of homeland security information) (codified as amended at 6 U.S.C. § 482).

Program Manager to plan for, oversee implementation of, and manage the ISE. Other duties and responsibilities of the Program Manager include assisting in the development of policies and issuing procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE, as well as monitoring and assessing its implementation. According to the Program Manager, the ISE is not intended to be a traditional, dedicated information system. Rather, in general, the ISE is to ensure—to the greatest extent practicable—a decentralized, distributed, and coordinated environment that builds upon existing systems and leverages ongoing efforts.

In January 2005, we designated information sharing for homeland security a high-risk area because the federal government faced formidable challenges in analyzing and disseminating this information in a timely, accurate, and useful manner.³ We reported that information is a crucial tool in fighting terrorism and that its timely dissemination is critical to maintaining the security of our nation. The federal government's sharing of terrorism-related information remained a high-risk area in our February 2011 update.⁴

In March 2006, we reported that the ISE had not yet been established.⁵ Subsequently, in November 2006, the Program Manager issued an implementation plan in accordance with the Intelligence Reform Act that provided an initial structure and approach for establishing the ISE, but acknowledged that further work was needed to fully define the ISE. In June 2008, we reported that the Program Manager had completed a number of tasks within the implementation plan and had included other information sharing initiatives in the ISE, but the plan did not include some important elements that were needed to implement the ISE, such as more fully defining and communicating the ISE's scope and communicating that information to stakeholders involved in the

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

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

⁵ See GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Procedures for Sharing Terrorism-Related and Sensitive but Unclassified Information*, [GAO-06-385](#) (Washington, D.C.: Mar. 17, 2006).

development of the ISE.⁶ We also reported that the desired results to be achieved by the ISE, including individual projects and specific milestones, had not yet been determined. We reported that these elements are essential in providing a road map, or program plan, to effectively implement the ISE.⁷ We recommended that the Program Manager and agencies more fully define the scope and specific results to be achieved by the ISE and develop performance measures to track progress. The Program Manager generally agreed and has taken some steps to address these recommendations but has not yet fully addressed them, as discussed later in this report.

In response to your request, this report updates our prior work and addresses to what extent the Program Manager for the ISE and key stakeholder agencies have (1) made progress in developing and implementing the ISE, and what work remains, and (2) defined an enterprise architecture (EA) to support ISE implementation efforts.⁸ The stakeholder agencies we reviewed are the five key agencies the Program Manager identified, consistent with the Intelligence Reform Act, as critical to developing and implementing the ISE—the Departments of Homeland Security (DHS), Justice (DOJ), State (State), and Defense (DOD), as well as the Office of the Director of National Intelligence (ODNI). These agencies represent five information sharing communities that collect the homeland security, law enforcement, foreign affairs, defense, and

⁶ See GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, [GAO-08-492](#) (Washington, D.C.: June 25, 2008).

⁷ According to Project Management Institute, *The Standard for Program Management*© (2006), a “roadmap” provides direction on how a program will be managed and defines its key variables.

⁸ An EA can be viewed as a reference or “blueprint” for achieving strategic business goals and outcomes, including maximizing information sharing within and across organization boundaries. A well-defined EA provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., homeland security) by documenting the entity’s current operational and technological environment and its target environment, as well as a plan for transitioning from the current to the target environment.

intelligence information deemed critical for sharing in order to provide for homeland security.⁹

To determine the extent to which the Program Manager and stakeholder agencies have made progress in developing and implementing the ISE, we reviewed relevant statutes and policies, including the Intelligence Reform Act and the 9/11 Commission Act. We also reviewed our prior reports and best practices identifying effective program management, federal coordination, and cost estimation.¹⁰ Through our review of these laws, guidance, and reports, we identified standards and best practices for program and project management and used them to inform our assessment of efforts to develop and implement the ISE and related efforts. We used semistructured interviews to gather information from the key agencies and facilitate analysis of their perspectives on the development of and remaining challenges impeding implementation of the ISE. We also used the interviews to obtain information from these agencies on the status of key activities the Program Manager identified as accomplishments in the 2009 and 2010 ISE annual reports to Congress, among other things.¹¹ In addition, we reviewed and analyzed agency guidance and plans for implementing the ISE and conducted interviews with officials from the key agencies to assess actions taken by the Program Manager to address recommendations in our 2008 report

⁹ In total, there are 15 ISE departments and agencies. In addition to the five key agencies (DHS, DOJ, State, DOD, and ODNI), the other 10 are the Central Intelligence Agency, the Department of Commerce, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Department of Transportation, the Department of the Treasury, the Federal Bureau of Investigation, the Joint Chiefs of Staff, and the National Counterterrorism Center.

¹⁰ See, for example, GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); Project Management Institute, *The Standard for Program Management* © (2006); GAO, *Determining Performance and Accountability Challenges and High Risks*, [GAO-01-159SP](#) (Washington, D.C.: November 2000); GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005); and GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).

¹¹ See Office of the Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment* (June 2009), and *Annual Report to the Congress on the Information Sharing Environment* (July 2010). See also U.S.C. § 485(h) (requiring the submission of annual performance management reports on the state of the ISE and information sharing across the federal government).

related to defining the purpose and scope of the ISE and the results to be achieved.

To determine the extent to which the Program Manager for the ISE and key stakeholder agencies have defined an EA to support ISE implementation efforts, we reviewed ISE architecture guidance and products prepared by the Office of the Program Manager—such as the *ISE Enterprise Architecture Framework* (EAF)¹²—and ISE architecture products prepared by the key ISE agencies, such as the DHS Information Sharing Segment Architecture.¹³ We then compared ISE architecture guidance and products against our prior reports and federal guidance on defining EA content and managing EA programs, including our Enterprise Architecture Management Maturity Framework (EAMMF) and the Office of Management and Budget (OMB) and the Federal Chief Information Officer Council’s *Federal Segment Architecture Methodology*.¹⁴ In addition, we interviewed officials from the Office of the Program Manager, key federal agencies, and OMB to obtain their perspectives on efforts to develop and manage an ISE EA. Appendix I provides additional details about our objective, scope, and methodology.

We conducted this performance audit from October 2009 through July 2011 in accordance with generally accepted government auditing standards.¹⁵ 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

¹² Office of the Program Manager, Information Sharing Environment, *ISE Enterprise Architecture Framework*, Version 2.0 (September 2008).

¹³ A segment architecture represents a portion of the overall enterprise that can be approached as a separate initiative under the overall EA.

¹⁴ See, for example, GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C.: August 2010), and Chief Information Officers Council Federal Segment Architecture Working Group and Office of Management and Budget, *Federal Segment Architecture Methodology* (December 2008).

¹⁵ This time frame reflects the fact that in June 2010, the President appointed the current Program Manager, and we needed time to assess his plans for moving forward with development of the ISE and to obtain perspectives from the five key ISE agencies on this change in leadership and on his plans. In the interim, we reported on preliminary results related to the overall review and the current Program Manager’s plans in our February 2011 high-risk update on the federal government’s sharing of terrorism-related information. See [GAO-11-278](#).

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

Background

Following the terrorist attacks of 2001, Congress and the executive branch took numerous actions aimed explicitly at establishing a range of new measures to strengthen the nation's ability to identify, detect, and deter terrorism-related activities and protect national assets and infrastructure from attack.¹⁶ One theme common to nearly all these efforts was the need to share timely information on terrorism-related matters with a variety of agencies across all levels of government. The ability to share security-related information can unify the efforts of federal, state, and local government agencies in preventing or minimizing terrorist attacks.

History of the Information Sharing Environment

Section 1016 of the Intelligence Reform Act, as amended by the 9/11 Commission Act, required the President to take action to facilitate the sharing of terrorism-related information by creating an information sharing environment—what has become the ISE. Consistent with the Intelligence Reform Act, the Program Manager intends for the ISE to provide the means for sharing terrorism information in a manner that—to the greatest extent practicable—ensures a decentralized, distributed, and coordinated environment that builds upon existing systems and leverages ongoing efforts. Under the act, the President is to designate a Program Manager to, among other things, plan for, oversee implementation of, and manage the ISE. The act also established an Information Sharing Council to assist the President and the Program Manager in carrying out these duties. Furthermore, 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 not later than 1 year after the date of

¹⁶ These 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 (Sept. 16, 2003) and 7 (Dec. 17, 2003), 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 enactment of legislation calling for, among other things, efforts to facilitate the sharing of terrorism-related information. See, for example, Pub. L. No. 108-458, § 1016, 118 Stat. at 3664-70 (mandating the creation of an information sharing environment), and Pub. L. No. 107-296, § 892, 116 Stat. at 2253-55 (mandating the implementation of procedures to facilitate the sharing of homeland security information).

enactment (enacted December 17, 2004) and specified elements to be included in this plan. These elements include, among other things, a description of the function, capabilities, resources, and conceptual design of the ISE; budget estimates; metrics and performance measures; and delineation of ISE stakeholder roles. The act also required the submission of annual performance management reports, beginning not later than 2 years after enactment, and annually thereafter, on the state of the ISE and on information sharing across the federal government.¹⁷

In April 2005, the President designated a Program Manager responsible for information sharing across the federal government, in accordance with the Intelligence Reform Act. In December 2005, the President issued a memorandum to implement measures consistent with establishing and supporting the ISE.¹⁸ The memorandum set forth information sharing guidelines, such as defining common standards for how information is to be acquired, accessed, shared, and used within the ISE and standardizing the procedures for handling sensitive but unclassified information. The memorandum also directed the heads of executive departments and agencies to actively work to promote a culture of information sharing within their respective agencies and reiterated the need to leverage ongoing information sharing efforts in the development of the ISE.

In November 2006, the Program Manager issued an ISE implementation plan to provide an initial structure and approach for ISE design and implementation.¹⁹ The plan incorporated the guidelines in the President's December 2005 memorandum as well as elements spelled out in the Intelligence Reform Act. For example, the plan included steps toward developing standardized procedures for handling sensitive but unclassified information as well as protecting information privacy, as called for in the President's information sharing guidelines. Under the plan, the ISE would consist of five "communities of interest"—homeland security, law enforcement, foreign affairs, defense, and intelligence. In

¹⁷ The first ISE annual report to Congress was released in September 2007.

¹⁸ See Presidential Memorandum, *Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment* (Dec. 16, 2005).

¹⁹ Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan*.

addition, in August 2007, the Program Manager issued the initial version of an EAF, which is intended to support ISE implementation efforts.

In October 2007, the President issued the *National Strategy for Information Sharing*.²⁰ The strategy focuses 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. The strategy notes that the ISE is intended to enable trusted partnerships among all levels of government in order to more effectively detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the United States. Further, according to the strategy, these partnerships should enable the trusted, secure, and appropriate exchange of terrorism-related information across the federal government; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications. 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 July 2009, the administration established the Information Sharing and Access Interagency Policy Committee (ISA IPC) within the Executive Office of the President to, among other things, identify information sharing priorities going forward.²¹ The committee—with representation of participating ISE agencies and communities—is intended to provide oversight and guidance to the ISE.²² In June 2010, the President appointed the current Program Manager and the White House designated the White House Senior Director for Information Sharing Policy and the

²⁰ The White House, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Terrorism Information Sharing* (Washington, D.C.: Oct. 31, 2007).

²¹ The ISA IPC assumed the functions and responsibilities of the former White House Information Sharing Council, which had been established pursuant to section 1016(g) of the Intelligence Reform Act. See 6 U.S.C. § 485(g).

²² The committee consists of representatives from the Central Intelligence Agency, Department of Agriculture, Department of Commerce, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of the Interior, Department of Justice, Department of State, Department of the Treasury, Department of Transportation, Federal Bureau of Investigation, Joint Chiefs of Staff, National Security Agency, Office of Management and Budget, Office of the Director of National Intelligence, and Office of the Secretary of Defense.

Program Manager co-chairs of the ISA IPC. The ISA IPC is responsible for advising the President and Program Manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE. Also, pursuant to the Intelligence Reform Act, the head of each department or agency that participates in the ISE is required to ensure compliance with information sharing policies, procedures, guidelines, rules, and standards. Further, OMB provides budgetary, programmatic, and architecture policy guidance to ISE agencies; prepares the President's budget; and measures performance.

The ISE is not a traditional, dedicated information system, according to the Program Manager. Rather, it is an interrelated set of policies, processes, and systems intended to allow ISE agencies to access and share information in a decentralized, distributed, and coordinated environment that builds upon existing systems and leverages ongoing efforts. The Program Manager also noted that the ISE is not a program in the traditional sense with a finite set of requirements, deliverables, and milestones and an agreed-to budget and manpower resources. Nevertheless, it is an effort that receives government funding and can be reviewed using program and project management principles.

Our Previous Reports on ISE Efforts

In June 2008, we reported that the Program Manager and stakeholder agencies had completed a number of tasks outlined in the 2006 implementation plan, including, among other things,

- 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—and
- the development of procedures and markings for sensitive but unclassified information to facilitate the exchange of information

among ISE participants.²³ Departments and agencies are in the process of determining how they will implement this guidance (once implemented, this effort could help improve access to information and therefore improve information sharing).

Nevertheless, we reported that the action items in the Program Manager's June 2006 implementation plan did not address all of the activities that must be completed to implement the ISE. For example, we noted that work remained in defining the ISE's scope and in determining all terrorism-related information that should be part of the ISE. Moreover, we found that the desired results to be achieved by the ISE—that is, how information sharing is to be improved, the individual projects and initiatives to achieve these results, and specific milestones—had not yet been determined. Thus, as previously discussed, we recommended, among other things, that the Program Manager 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. The Program Manager and agencies have taken some steps to address this recommendation but have not yet fully addressed it, as we discuss later in this report.

The sharing of terrorism-related information remains on our high-risk list.²⁴ Our work in this area has consistently focused on how well the federal government is sharing information among federal agencies as well as with state, local, tribal, private sector, and international partners. As such, our focus has been on progress the federal government has made in standing up the ISE. In February 2011, we reported that while the federal government has continued to make progress in sharing terrorism-related information among its many partners, it does not yet have a fully functioning ISE in place.

²³ In March 2006, we reported 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. Consistent with our recommendations, agencies have begun taking actions to develop policies, procedures, and controls for handling sensitive but unclassified information. See [GAO-06-385](#). See also, Exec. Order No. 13,566, *Controlled Unclassified Information*, 75 Fed. Reg. 68,675 (Nov. 9, 2010) (establishing an open and uniform program for managing information that requires safeguarding or dissemination controls).

²⁴ [GAO-11-278](#).

Program Manager and Agencies Have Advanced Key Information Sharing Activities but Have Not Yet Developed a Comprehensive Road Map to Effectively Implement the ISE

Since we issued our 2008 report, the Program Manager and agencies have established a discrete set of goals and undertaken activities to guide development and implementation of the ISE, but these actions do not fully address our recommendations or provide the comprehensive road map that we called for in our report. For example, the Program Manager and agencies have not yet fully defined what the ISE is expected to achieve and contain, identified the incremental costs necessary to implement the ISE, or fully developed procedures to show what work remains and related milestones to provide accountability for results. The administration has taken steps to strengthen the ISE governance structure to help guide the development and implementation of the ISE, but it is too early to gauge the structure's effectiveness.

The Program Manager and Agencies Have Established a Discrete Set of Goals and Undertaken Activities under the ISE, but Work Remains in Developing and Implementing the ISE

In November 2006 and in accordance with the Intelligence Reform Act, the Program Manager submitted an ISE implementation plan to Congress that, according to the plan, was intended to help guide development of the ISE for a 3-year period. The plan addressed initial actions for defining the ISE as well as agency responsibilities and time frames. However, as we discussed in our 2008 report, the plan did not include some important elements needed to develop and implement the ISE. Work remained 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.

Subsequently, in part based on recommendations made in our 2008 report, the Program Manager worked with the five key agencies to create a new plan to guide development of the ISE, which they called an ISE "framework." Specifically, the framework identified four goals for the ISE, which were to (1) create a culture of sharing; (2) reduce barriers to sharing; (3) improve information sharing practices with federal, state, local, tribal, and foreign partners; and (4) institutionalize sharing. The framework also identified 14 specific subgoals or activities agencies were to pursue. Some of these activities were intended to institutionalize information sharing practices into agency operations, such as establishing information sharing and incentive programs for federal employees. For example, DHS, DOJ, and DOD, as well as ODNI have made information sharing a factor in their incentives programs by offering employees awards based on their contributions to information sharing and collaboration practices. The framework also cataloged agencies' ongoing information sharing initiatives to leverage their benefits across the

government, consistent with the Intelligence Reform Act, including the following:²⁵

- **The Nationwide Suspicious Activity Reporting Initiative.**²⁶ This initiative builds on what state and local law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents indicative of criminal activity that may be precursors to terrorism—and establishes a standardized process to share this information among agencies to help detect and prevent terrorism-related activity. In February 2010, DOJ became the lead agency for the initiative and established a program management office to support its development in cooperation and coordination with DHS and the Federal Bureau of Investigation.
- **The national network of fusion centers.** This initiative is designed to leverage the fusion centers that all 50 states and some major urban areas have established to address gaps in terrorism-related information sharing that the federal government cannot address alone and provide a conduit for information sharing within each state, among other things.²⁷ In 2010, federal, state, and local officials from across the country launched the first nationwide assessment of fusion center capabilities, with the goal of helping centers close gaps so they have a consistent baseline of information sharing capabilities. Information from this assessment is to be used to develop strategies and realign resources to close those gaps going forward.²⁸

²⁵ In addition to the 14 specific subgoals under the ISE framework, the Program Manager noted that other components of the ISE include the National Information Exchange Model as well as other efforts focused on sharing unclassified and classified information. The National Information Exchange Model is a federal, state, local, and tribal interagency initiative that is intended to provide the foundation for the seamless exchange of information across departments and agencies by encouraging participating organizations to format data in a consistent manner.

²⁶ In general, suspicious activity is defined as observed behavior or incidents that may be indicative of intelligence gathering or preoperational planning related to terrorism, crime, espionage, or other illicit intentions.

²⁷ In general, fusion centers are collaborative efforts of two or more agencies that provide resources, expertise, and information to the centers with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

²⁸ GAO, *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, [GAO-10-972](#) (Washington, D.C.: Sept. 29, 2010).

-
- **ISE privacy and civil liberties.** ISE stakeholders have made an effort to strengthen privacy, civil rights, and civil liberties across all sectors of the ISE. According to the July 2010 annual report, 9 of 15 ISE stakeholders had implemented ISE privacy policies. These policies are intended to ensure that privacy and other legal rights of Americans are protected in the development and use of the ISE.

For the subgoals in the framework, the Program Manager established a process to gauge and track agencies' progress in implementing these subgoals and a related set of performance measures. The Program Manager included the framework in both the June 2009 and July 2010 annual progress reports to Congress. As discussed later in this report, the framework and annual reports to Congress did not specifically address what work remained in completing the initiatives or related milestones.

The ISE framework has served as a plan to guide development of the ISE and its discrete set of 14 subgoals. The framework includes a number of elements that our work has shown are important for developing and implementing broad, crosscutting initiatives like the ISE, such as defined goals, objectives, activities, and metrics. However, as discussed in more detail later in this report—in part because the framework is limited to these 14 subgoals and does not define what the fully functioning ISE is to achieve and include—it does not provide the comprehensive road map that is needed to further develop and implement the ISE going forward. In April 2010, the White House Senior Director for Information Sharing Policy acknowledged that the ISE framework is a set of 14 disparate activities that do not constitute a governmentwide initiative to share terrorism information, as envisioned by the Intelligence Reform Act. According to the Program Manager, the role of the current framework in guiding further development of the ISE and the extent to which other activities will be integrated into the framework have not yet been determined. Therefore, it is unclear how, if at all, the framework and its related goals and activities will be used to guide future development of the ISE.²⁹

²⁹ App. II contains additional information on the ISE framework.

More Fully Defining the ISE, Related Costs, and What Work Remains Could Help to Facilitate Implementation and Accountability for Results

More than 6 years after enactment of the Intelligence Reform Act and initial efforts to create the ISE, there is not a clear definition of what the ISE is intended to achieve and include. The Program Manager and ISE agencies have ongoing efforts to more fully define this “end state” vision, which is a key next step for ISE development, by the end of summer 2011. After this vision is defined, it will be important for the Program Manager and ISE agencies to ensure that all relevant agency initiatives are leveraged by the ISE to improve information sharing across all communities and to define the incremental costs related to implementing the ISE so agencies can determine how to fund future investments. The Program Manager has enhanced monitoring of ISE initiatives, but additional actions could help demonstrate progress and provide accountability for results. In addition to Intelligence Reform Act requirements, our prior work has found that these activities help to provide a road map for responsible parties in developing and implementing broad, crosscutting initiatives like the ISE.³⁰ Such actions are also consistent with criteria we use to assess whether agencies have made progress to resolve past terrorism-related information sharing problems, thereby reducing the risk that these problems pose to homeland security.³¹

The Program Manager Has Ongoing Efforts to Define What the ISE Is Intended to Achieve and Include, Which Is a Key Next Step for ISE Development

A road map for the ISE should identify key next steps for ISE development and start with a clear definition of what the ISE is intended to achieve and include—or the “end state” vision. In 2008, we reported that while the Program Manager had completed a plan with an initial structure and approach for ISE design and implementation, he had not yet determined the desired results to be achieved by the ISE, and we recommended that he do so, among other things. The Program Manager has also acknowledged the importance of developing an end state vision for the ISE and noted that he is doing so as part of efforts to update the 2007 *National Strategy for Information Sharing*. The Program Manager said that this update will drive future ISE implementation efforts and will help individual agencies across all five communities adapt their information sharing policies, related business processes, architectures, standards, and systems to effectively operate with the ISE.

³⁰ See, for example, [GAO-04-408T](#).

³¹ [GAO-01-159SP](#).

According to the Program Manager, the end state vision will define the current state of the ISE and the future vision to be achieved by agencies as they work to further develop and implement the ISE. DHS and DOJ officials we contacted also cited the importance of developing an end state vision to assist in guiding development and implementation of the ISE. For example, DOJ officials stated that a defined end state would facilitate development and implementation of common goals going forward.

The Program Manager has publicly acknowledged the need to accelerate ISE progress. To inform efforts to define an end state vision, the Program Manager has been soliciting ideas and input from ISE stakeholder agencies. According to the Program Manager, the updated *National Strategy for Information Sharing* and the ISE end state vision have not been finalized, and therefore it is premature to speculate on questions such as changes in program or investment priorities as well as information sharing gaps and challenges to be addressed. In June 2011, the Program Manager said that the national strategy will be updated in the near future, but he did not provide a specific date.

According to the Program Manager, the end state vision will be a snapshot at a point in time because as threats continue to evolve, the ISE will need to evolve as well. The Program Manager noted that after development of the end state vision is completed, supporting implementation plans will be needed to help guide achievement of the vision, including plans that define what activities and initiatives will be needed to achieve the end state and to guide development and implementation of the ISE. Such plans would be consistent with our call for a road map, if they contain key ingredients such as roles, responsibilities, and time frames for these activities, among other things. Further, as we discuss later in this report, the process of defining an EA for the ISE—and agencies' associated segment architectures that support their individual ISE activities—could help the Program Manager and agencies in their efforts to define the current operational and technological capabilities within the ISE, the future capabilities needed, and a plan to transition between the two.

Ensuring That All Relevant Agency Initiatives Are Leveraged by the ISE Could Enhance Information Sharing Governmentwide

The September 11, 2001, terrorist attacks exposed that the five ISE communities—homeland security, law enforcement, foreign affairs, defense, and intelligence—were insulated from one another, which resulted in gaps in the sharing of information across all levels of government.³² Before the attacks, the overall management of information sharing activities among government agencies and between the public and private sectors lacked priority, proper organization, coordination, and facilitation. Consistent with the Intelligence Reform Act, the ISE is intended to provide the means for sharing terrorism information across the five communities in a manner that, among other things, builds upon existing systems and leverages ongoing efforts. To date, the ISE has primarily focused on the homeland security and law enforcement communities and related sharing between the federal government and state and local partners, in part to align with information sharing priorities.

OMB ISE programmatic guidance shows that ISE activities have been primarily focused on sharing within the homeland security and law enforcement communities and with domestic partners—such as state and local law enforcement agencies. This guidance—developed in collaboration with ISE leadership—outlines the White House’s priorities for the ISE and those that agencies are to focus on and align resources and investments to during a given fiscal year. For fiscal year 2012, OMB’s programmatic guidance identifies the following priorities, which are primarily focused on sharing information between the federal government and state and local partners:

- building a national integrated network of fusion centers,
- continuing implementation of the Nationwide Suspicious Activity Reporting Initiative,
- establishing Sensitive but Unclassified/Controlled Unclassified Information network interoperability,
- improving governance of the Classified National Security Information Program,³³ and
- advancing the implementation of controlled unclassified information policy.

³² The White House, *National Strategy for Information Sharing*.

³³ The Classified National Security Information Program is designed to safeguard and govern access to classified national security information shared by the federal government with state, local, tribal, and private sector entities.

Officials from all five communities generally agreed that ISE activities undertaken to date have been primarily focused on sharing within the homeland security and law enforcement communities—primarily domestic sharing between the federal government and state, local, and tribal partners. According to DOJ officials, this initial focus was appropriate and allowed the Program Manager to leverage agencies’ ongoing efforts to share terrorism-related information. The officials noted that by focusing on a select set of initiatives—such as the Nationwide Suspicious Activity Reporting Initiative and the national network of fusion centers—the Program Manager was able to make progress toward implementing ISE priorities. We recognize that recent homeland security incidents and the changing nature of domestic threats make continued progress in improving sharing between federal, state, and local partners critical.³⁴ However, consistent with the Intelligence Reform Act, the ISE is intended to provide the means for sharing terrorism information across all five communities.

The Program Manager and ISE agencies have not yet ensured that initiatives within the foreign affairs, defense, and intelligence communities have been fully leveraged by the ISE to enhance information sharing within and across all communities. According to State officials, the department shares terrorism-related information with other agencies through a variety of efforts and initiatives related to national and homeland security. The officials noted that most of the initiatives are non-ISE efforts, meaning that they did not originate in the Program Manager’s office. The officials also noted that the department has only been asked to provide one kind of terrorism-related information as part of one ISE initiative related to Suspicious Activity Reporting and complied with this request. According to the Program Manager, State also possesses information about entrants to the country that could be valuable to the ISE. However, in April 2011, State officials said that the Office of the Program Manager has not contacted the department’s coordinator for the ISE to request information on programs or initiatives related to people entering the country. Therefore, the Program Manager and State have not determined if this information could be used to benefit other ISE communities. DOD officials also said that the department is undertaking activities outside of the ISE, such as efforts to develop interagency agreements between DOD and the Federal Bureau of Investigation for

³⁴ [GAO-11-278](#).

the purpose of sharing terrorism-related information. According to DOD officials, this effort could be part of the ISE if the information addressed within these agreements is consistent with the ISE's established standards, among other things.

In addition, the December 25, 2009, attempted terrorist attack highlighted the importance of effective information sharing within the intelligence community and demonstrated the potential consequences if information is not shared in a manner that facilitates its use in analysis, investigations, and operations. The intelligence community's efforts to better share classified information among intelligence agencies are highlighted in the 2010 annual report, but the report does not discuss the extent to which these initiatives are being coordinated within and among the five communities or how the ISE could leverage their benefits. For example, the report discusses an initiative that will allow intelligence community personnel to search for or discover information, including terrorism-related information, across all agencies within the community.³⁵ According to the Program Manager, this ODNI initiative—while so far limited to the intelligence community—should be highlighted as a best practice across the ISE. However, the 2010 report does not discuss whether and how these technological advances could be used to benefit other communities or how they are implementing this best practice. Also, according to the Program Manager, the ISE has generally left the sharing of Top Secret and higher information to ODNI and intelligence community agencies since they manage most of this information. He said that this was unlikely to change significantly in the future. Ensuring that the intelligence community is fully involved in developing the ISE could help resolve the problems the September 11 attacks exposed—especially that critical information was contained in agencies' individual stovepipes and not shared.

Further, in part because of the focus on domestic sharing with the homeland security and law enforcement communities, not all agencies have been similarly engaged in building the ISE or have had their initiatives leveraged as discussed above. Officials from the five key agencies said that they have actively participated in ISA IPC meetings and have had opportunities to provide feedback on emerging policy

³⁵ Office of the Director of National Intelligence, Intelligence Community Directive Number 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* (Jan. 21, 2009).

decisions. They also noted that when appropriate, they participate in the development and implementation of OMB priorities and initiatives set forth by the ISA IPC and Program Manager. However, State, DOD, and ODNI officials also reported that development of the ISE has had limited focus to date on information sharing within and among the foreign affairs, defense, and intelligence communities.

State officials said that the ISE priorities established to date generally do not engage State's mission because the initiatives are primarily focused on sharing with state and local partners, while State's mission focuses on building relationships within the foreign affairs community. Similarly, DOD officials said they have been engaged in some ISE priorities—such as implementing the Nationwide Suspicious Activity Reporting Initiative—but that DOD has not been tasked to lead any new terrorism-related information sharing initiatives. In addition, ODNI officials said that because many ISE activities are focused on efforts with state, local, tribal, and private sector partners, the intelligence community's participation in those activities is limited as the intelligence community, by mission and statute, primarily focuses on foreign intelligence.

The Program Manager acknowledged that the most visible outcomes of the ISE have been in the law enforcement and homeland security communities. However, he noted that officials from the Office of the Program Manager have worked with State to standardize terrorism-related information sharing agreements with foreign governments; worked with DOJ and DOD to develop information technology standards that allow different agencies to exchange information; and worked with ODNI and the intelligence community to develop terrorism-related information products for state, local, and tribal governments. The Program Manager also noted that State, DOD, and ODNI are participants in the ISA IPC and have been afforded opportunities to help set ISE programmatic priorities and participate in discussions and decisions about where to strategically prioritize scarce resources. Nevertheless, the Program Manager has also recognized the need to enhance and extend partnerships across all five communities and said that significant outreach to ISE agencies has been under way since he became Program Manager in July 2010. In addition to his outreach efforts, the Program Manager has suggested that specific agencies—such as State, DOD, and ODNI—could also develop proposals for how their information sharing activities could be better integrated into the ISE.

Consistent with the Intelligence Reform Act, the ISE is intended to provide the means for sharing terrorism information across all five communities in

Defining Incremental Costs
Necessary to Implement the
ISE Would Allow Decision
Makers to Plan for and
Prioritize Future Investments

a manner that builds upon existing systems and leverages ongoing efforts. After the end state vision is defined, taking actions to ensure that all relevant information sharing initiatives across the five communities are fully leveraged could help the Program Manager and ISE agencies enhance information sharing governmentwide and better enable the federal government to share information that could deter or prevent potential terrorist attacks.

Section 1016 of the Intelligence Reform Act required the President, with the assistance of the Program Manager, to include as part of the ISE's implementation plan, a budget estimate that identified the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE. In June 2008, we reported that the initial ISE Implementation Plan issued in 2006 did not provide a budget estimate that identified incremental costs in accordance with the act, but that the Program Manager indicated that steps to develop such an estimate would be taken in the future.³⁶ At that time, a budget estimate that identified incremental costs had not been developed, in part, because the ISE was in such an early stage of development and it would have been difficult for agencies to know what to include in developing such a cost estimate. The Program Manager, in the 2009 ISE annual progress report, also identified the need to coordinate investments for terrorism-related initiatives as both a priority and a challenge, but noted that limited progress had been made in defining the resources needed to implement the ISE. The 2010 annual progress report noted that the Office of the Program Manager had developed a process that is intended to link ISE initiatives and performance measures to investment decisions. However, the Program Manager could not identify the level of investments that have been dedicated to the ISE to date. The Program Manager also could not identify the future incremental investments needed to develop and implement the ISE, in part because the Program Manager and key agencies had not yet determined what the ISE is to achieve and include.

Officials from the Office of the Program Manager said they had not prepared estimated costs for the ISE and that there has never been a stand-alone budget for the program. The officials said that because the ultimate goal of the ISE is to become an institutionalized practice among agencies, to separate or designate funding for ISE-related activities as

³⁶ [GAO-08-492](#).

part of agency budget processes would undermine this overarching goal. Further, OMB officials said that because information sharing is a core mission of all departments and agencies, they are to cover costs to implement information sharing initiatives from within their existing budgets. Nevertheless, while an estimate has not been prepared, the Program Manager said that progress has been made in collecting certain ISE-related costs. Specifically, OMB, in cooperation with the Office of the Program Manager, modified OMB Circular A-11 in 2010 to collect more information from agencies about planned ISE-related technology investments.³⁷ This effort is intended to identify costs related to agencies' information technology system investments, but it does not identify other types of incremental costs associated with implementing the ISE, such as those involving training and other administrative programs and activities. The Deputy Program Manager acknowledged the importance of identifying such incremental costs but noted that ISE agencies are best positioned to establish this cost and budget information.

Two of five agencies that we contacted noted that governmentwide initiatives, such as the ISE, are often difficult to implement without dedicated funding for mandated programs. For example, State officials noted that the department had challenges redirecting operational funds to achieve ISE program objectives during fiscal years 2008 and 2009. DOJ officials also acknowledged the challenges in implementing new governmentwide efforts without related funding, but noted that the use of "seed funding" in support of key terrorism-related information sharing initiatives—such as the Nationwide Suspicious Activity Reporting Initiative and fusion center programs—has been one of the major successes of the ISE.³⁸

We recognize that attaining accurate and reliable incremental cost estimates for the ISE is a difficult undertaking, complicated further by the fact that the Program Manager and agencies are still defining what the

³⁷ OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, July 2010.

³⁸ While agencies are to cover costs to implement information sharing initiatives from within their existing budgets, to help agencies, the Office of the Program Manager for the ISE provides "seed funding" from its budget for governmentwide ISE initiatives. According to the Program Manager, approximately \$8.9 million, or 37 percent of the office's 2010 budget, estimated by OMB officials to be \$24 million, was made available for seed funding. The Office of the Program Manager for the ISE is funded through amounts appropriated to ODNI.

The Program Manager Has Enhanced Monitoring of ISE Initiatives, but Additional Actions Could Help Demonstrate Progress and Provide Accountability for Results

ISE is, is to include, and is to attain. However, new ISE requirements will need additional investments, regardless of whether they are funded through existing agency budgets, a separate program budget, or another mechanism. Our best practices on cost estimation note that the ability of agencies to generate reliable cost estimates is a critical function for effective program management. In addition, our prior work shows that cost information can help agencies allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate.³⁹ After the ISE end state vision is defined and needed activities and initiatives are identified, developing incremental cost estimates would help agencies plan and budget for these activities and initiatives and allow Congress and other decision makers to prioritize future investments and demonstrate a continued commitment to supporting the ISE.

The Intelligence Reform Act requires the Program Manager to, among other things, monitor implementation of the ISE by federal departments and agencies to ensure that adequate progress is being made and regularly report the findings to Congress. In June 2008, we reported that the Office of the Program Manager was monitoring ISE implementation—as demonstrated through its September 2007 annual report to Congress—but that such monitoring did not include an overall assessment of progress in implementing the ISE and how much work remained. Thus, we recommended, among other things, that the Program Manager (1) develop a way to measure and demonstrate results to ensure that the ISE was on a measurable track to success and to show the extent to which the ISE had been implemented and what work remained and (2) more fully define the key milestones needed to achieve ISE results.⁴⁰ The Program Manager generally agreed and has taken some steps to address these recommendations but has not yet fully addressed them. These practices are critical to an effective monitoring system and would help to provide an accurate accounting for progress to Congress and other stakeholders. Further, our prior work on high-risk issues shows that agencies must have a way to monitor and demonstrate progress against baseline requirements—in this case, the activities, milestones, and results to be achieved for the ISE.

³⁹ [GAO-04-408T](#).

⁴⁰ [GAO-08-492](#).

The Program Manager has taken steps to address our recommendations by instituting a “maturity model” to monitor and track progress. For example, the maturity model tracks each of the 14 initiatives in the ISE framework from their early stages of development until they are considered to be institutionalized into agency operations. The model contains four levels:

- *Ad-hoc*: Information sharing occurs among functions or groups with few repeatable processes.
- *Defined*: Information sharing sources and products are identified and processes are followed.
- *Managed*: Information sharing is well characterized and consistently performed across organizational boundaries.
- *Institutionalized*: Information sharing is quantitatively managed and business processes are aligned, seeking continuous improvement.

In the July 2010 annual report to Congress, the Program Manager noted that 9 of the 14 initiatives were at the second level and had been “defined,” and the remaining 5 were at level three and being “managed.” The maturity model and related reporting provide useful information on the status of ISE initiatives and provide a general indicator of the overall progress of the ISE. Nevertheless, these actions do not fully address our recommendations because the annual reports do not specifically address what work remains in completing the 14 initiatives or related milestones for completion, which are important elements in determining overall progress in implementing the ISE and establishing accountability for future efforts. The Program Manager’s ongoing efforts to define the ISE end state vision and implementing road map—to the extent that they include associated time frames and milestones for achieving both individual projects or activities as we recommended in June 2008 as well as the capabilities of a fully implemented ISE as envisioned—would help to provide a baseline for decision makers and investors to measure ISE progress. This baseline could be used to determine what work has been achieved and remains and whether additional efforts to accelerate progress are needed, among other things.

While the framework did not establish time frames or milestones, the Office of the Program Manager uses an annual performance questionnaire to collect information on the agencies’ progress in implementing 10 of the 14 initiatives to inform the maturity model. According to officials from the Office of the Program Manager, the survey does not include data on the other 4 initiatives—the Nationwide

Suspicious Activity Reporting Initiative, fusion centers, efforts to standardize controlled unclassified information, and the Interagency Threat Assessment and Coordination Group.⁴¹ Instead, the officials said that each of the agencies with responsibility for leading these efforts monitors its own performance to ensure progress and provides a summary of progress highlights to the Office of the Program Manager, which is incorporated into the annual report. For example, the 2010 annual report highlighted the successful integration of a Federal Bureau of Investigation system into the Nationwide Suspicious Activity Reporting Initiative. These summaries provide information that shows what agencies are doing and demonstrate recent accomplishments, but they do not provide a gauge to measure progress achieved versus what work remains or milestones for completing remaining work regarding fully developing and implementing the ISE.

In January 2011, the ISA IPC and the Office of the Program Manager initiated an effort to make ISE priority programs and related goals more transparent and to better monitor progress. Specifically, according to the Deputy Program Manager, agencies that are responsible for implementing ISE priority programs are leading efforts to establish 3-, 6-, and 12-month goals for these programs. He noted that once the goal-setting process is established, information on progress made in reaching these goals may be included in future ISE annual reports. This process should help to provide accountability over ISE priority programs on a yearly basis.

The 2008, 2009, and 2010 annual reports to Congress include some performance measures, such as the number of departments and agencies that have conducted ISE-related awareness training or have developed and implemented ISE privacy policies. Including these measures in annual reports is an important step in providing accountability for results, but it does not fully address our recommendation because the measures generally focus on counting activities (i.e., output measures) accomplished rather than results

⁴¹ The Interagency Threat Assessment and Coordination Group is a group of state, local, tribal, and federal homeland security, law enforcement, and intelligence officers at the National Counterterrorism Center—the federal government’s primary entity for integrating and analyzing intelligence on international terrorists—that reviews federal reports and provides counsel and subject matter expertise in order to better meet the information needs of state, local, tribal, and private entities.

achieved (i.e., outcome measures), such as how and to what extent sharing has been improved and ultimately, to the extent possible, what difference these improvements are making in helping to prevent terrorist attacks. The Deputy Program Manager stated that the Office of the Program Manager recognizes the need to develop performance measures that show how and to what extent sharing has been improved and that the goal-setting process should assist in transitioning from output to outcome-oriented performance measures.

We recognize and have reported that it is difficult to develop performance measures that show how certain information sharing efforts have affected homeland security.⁴² Nevertheless, we have recommended that agencies take steps toward establishing such measures to hold them accountable for the investments they make. We also recognize that agencies may need to evolve from relatively easier output measures—that for example count the number of agencies that have conducted ISE-related awareness training—to more meaningful measures that weigh agencies' satisfaction with the timeliness, usefulness, and accuracy of information shared until the agencies can establish outcome measures that determine what difference the information made to federal, state, local, and other homeland security efforts. Thus, we continue to believe that our June 2008 recommendation to the Program Manager and key agencies to develop performance measures that show the extent to which the ISE has been implemented and sharing improved has merit and should be fully implemented.

⁴² See, for example, GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, [GAO-09-399](#) (Washington, D.C.: Sept. 30, 2009), and *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, [GAO-07-454](#) (Washington, D.C.: Aug. 17, 2007).

The Administration Has Taken Steps to Strengthen the ISE Governance Structure, but It Is Too Early to Gauge the Structure's Effectiveness

Our prior work on high-risk issues shows that a strong commitment from top leadership to addressing problems and barriers to sharing terrorism-related information is important to reducing related risks. In July 2009, the White House established the ISA IPC within the Executive Office of the President to subsume the role of its predecessor interagency body—the Information Sharing Council.⁴³ The Assistant to the President for Homeland Security and Counterterrorism designated the White House Senior Director for Information Sharing Policy to chair the new committee. These changes were intended to bring high-level policy decision making and oversight to the development of the ISE.

The Intelligence Reform Act requires the Program Manager to plan for, manage, and oversee implementation of the ISE, including assisting in the development of policies to guide implementation and ensure progress. In a July 2009 testimony, the Program Manager at that time cited concerns about the Program Manager's authority and provided recommendations intended to help strengthen the ISE effort.⁴⁴ For example, among other things, he recommended having a presidential appointee serve as Program Manager and having the Program Manager co-chair the ISA IPC. Following this Program Manager's resignation, an acting Program Manager assumed responsibility for implementing the ISE until June 2010, at which time the President appointed the current Program Manager. Also, in June 2010, the Assistant to the President for Homeland Security and Counterterrorism designated the Program Manager as a co-chair of the ISA IPC—along with the White House Senior Director for Information Sharing Policy—which was consistent with the prior Program Manager's recommendations. According to the Office of the Program Manager, having the Program Manager for the ISE also co-chair the ISA IPC was intended to acknowledge that policies, business practices, architectures, standards, and systems developed for the ISE can be applicable to other types of national security information beyond

⁴³ The Information Sharing Council—composed of senior representatives from federal departments and agencies, some of whom 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.

⁴⁴ *Beyond ISE Implementation: Exploring the Way Forward for Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. 5 (2009) (statement of Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence).

terrorism and vice versa. In this role, the Program Manager is to ensure the close alignment of the ISE and broader national security information sharing activities.

The new Program Manager stated that he would have one of four levels of involvement in implementing the specific activities listed in the 2010 annual progress report to Congress:

- *Monitoring*: For certain information sharing activities that agencies are generally implementing on their own initiative, the Office of the Program Manager is to stay informed of ongoing developments to determine whether the activity might be a potential best practice that is applicable to other ISE mission partners. The Program Manager also monitors activities to stay abreast of issues that might eventually surface through the ISE process. For example, the Program Manager said he monitors the intelligence community's efforts to better share classified information among intelligence agencies.
- *Advising*: For some agency initiatives, the Program Manager said that the Office of the Program Manager may be called on to provide specialized information sharing expertise, even though the office is not responsible for actual implementation. For example, the Program Manager said his office has an advisory role in supporting the Nationwide Suspicious Activity Reporting Initiative.
- *Supporting*: For selected activities with significant implications for the ISE, the Program Manager said that the Office of the Program Manager is to play a more active support role, that this support could take many forms, and that it may include co-investment of seed capital in the early stages of specific high-priority efforts. For example, the Program Manager said the office supports agencies' efforts to designate and share controlled unclassified information.
- *Leading*: The Program Manager also said there are several activities for the ISE as a whole where the Office of the Program Manager is to take the lead role, providing the financial and personnel resources necessary to carry them out. For example, the Program Manager said the office has the lead role in providing communications and outreach related to the ISE.

The Program Manager also noted that his role could evolve as activities mature, as it did for the Nationwide Suspicious Activity Reporting Initiative.

The administration's steps to strengthen the ISE governance structure address concerns the prior Program Manager identified and our criteria for committed leadership. However, it is too early to tell how the new structure will affect the continued development and implementation of the ISE and if the Program Manager's new role will provide him sufficient leverage and authority to ensure that agencies consistently implement information sharing improvements governmentwide.

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

The Program Manager's 2010 annual report to Congress states that the office's architecture program for the ISE describes the rules and practices needed for planning and operating ISE systems consistent with EA best practices. According to relevant guidance,⁴⁵ an EA, or modernization blueprint, should include descriptions (i.e., "architecture views") of an enterprise's current and future environment for business processes, data and information, applications and services, technology, and security in meaningful models, diagrams, and narrative.⁴⁶ In addition, our Enterprise Architecture Management Maturity Framework (EAMMF) recognizes that various approaches for structuring an EA exist and can be applied to the extent that they are relevant and appropriate for a given enterprise. These approaches generally provide for breaking down an enterprise into its logical parts and allowing various components of an enterprise (e.g., ISE mission partners) to develop their respective parts of the EA in relation to enterprisewide needs and the inherent relationships and dependencies that exist among the parts.⁴⁷ Accordingly, our EAMMF provides flexibility for how such an EA should be developed and does not prescribe a

⁴⁵ See, for example, [GAO-10-846G](#); Chief Information Officer Council, Federal Enterprise Architecture Program Management Office, *The Federal Enterprise Architecture Security and Privacy Profile*, Version 2.0 (June 1, 2006); Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); and OMB Circular A-130, Revised (Transmittal Memorandum No. 4), Memorandum for Heads of Executive Departments and Agencies on Management of Federal Information Resources.

⁴⁶ Information included in an EA includes, among other things, business process models that describe the business activities (or tasks) performed and the information flows among these activities; data models that describe the data needed to support the business needs, the meaning and structure of the data, and how the data are to be made available; and technical reference models that describe the technical standards and technologies that are to be used in implementing enterprise application systems and services.

⁴⁷ For example, under a federated approach, member architectures (e.g., component, subordinate, or subsidiary architectures) are substantially autonomous, but they also inherit certain rules, policies, procedures, and services from the parent architecture.

specific approach by which organizations should develop EA content. In addition to providing descriptions of an enterprise's current and future environment, relevant guidance states that an EA should include an enterprise sequencing plan for transitioning from the current environment to the future environment. Specifically, the enterprise sequencing plan should describe an incremental strategy that includes scheduling multiple, concurrent, interdependent activities and incremental implementation to evolve the enterprise.

We have previously reported that successfully managing the development and implementation of an EA depends in large part on the extent to which effective management controls (e.g., policies, structures, processes, and practices) are employed.⁴⁸ Our EAMMF provides a benchmark against which to measure the extent to which a given enterprise is effectively managing its architecture program.⁴⁹ It defines various stages of maturity for an EA and the management controls expected to be in place for each stage.⁵⁰ Stages 1 and 2 of this framework can be viewed as providing for the institutional leadership and foundational management capabilities for the later stages to build upon and thereby achieve program success. For example, in stage 1 an enterprise commits to developing an EA and defines the purpose of its EA, and in stage 2 it defines the methodology and plans by which EA products are to be developed and maintained. An EA program that has not satisfied key stage 1 and 2 core elements can

⁴⁸ See, for example, GAO, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, [GAO-06-831](#) (Washington, D.C.: Aug. 14, 2006); *Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts*, [GAO-05-266](#) (Washington, D.C.: Apr. 29, 2005); and *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, [GAO-04-43](#) (Washington, D.C.: Nov. 21, 2003).

⁴⁹ [GAO-10-846G](#).

⁵⁰ The EAMMF is made up of seven stages of EA management maturity. Each stage reflects those management conditions that an enterprise should meet to logically build on the EA management capability established at the preceding stage, and to position it for introducing the EA management capability applicable to the next stage. Stage 0 involves creating EA awareness and does not include any specific core elements, stage 1 involves establishing EA institutional commitment and direction, stage 2 involves creating the management foundation for EA development and use, stage 3 involves developing initial EA versions, stage 4 focuses on completing and using an initial EA version for targeted results, stage 5 addresses expanding and evolving the EA and its use for institutional transformation, and stage 6 addresses continuously improving the EA and its use to achieve corporate optimization.

be considered ad hoc, unstructured, and unlikely to succeed. It is important to note that the EAMMF should not be viewed as either a rigidly applied checklist or as the only relevant benchmark for managing and assessing an EA program. Instead, it is intended to be applied flexibly with discretion in light of each enterprise's unique facts and circumstances.

The Program Manager has developed architecture guidance to assist in the implementation of the ISE. For example, in August 2007, Version 1.0 of the ISE EAF was released and in September 2008 it was revised.⁵¹ The framework is to provide strategic guidance to enable long-term business and technology standardization and information systems planning, investing, and integration in the ISE by documenting and organizing the ISE mission business goals and processes, services, data, and technologies and other operational capabilities necessary to facilitate information sharing. In addition, in May 2008 the Office of the Program Manager issued its *Profile and Architecture Implementation Strategy* (PAIS) to augment its ISE EAF and in June 2009 it was revised.⁵² Among other things, the PAIS describes a series of steps that the ISE agencies are to follow when developing their information sharing segment architectures⁵³ to support the implementation of ISE capability. These steps are generally consistent with federal guidance, such as the federal Chief Information Officers Council's *Federal Segment Architecture Methodology*.⁵⁴

The Program Manager and ISE agencies have also begun to develop products that describe several components of an ISE EA. For example, the Program Manager has worked with ISE agencies to establish cross-agency ISE segment architectures, such as the ISE Suspicious Activity

⁵¹ Office of the Program Manager, Information Sharing Environment, *ISE Enterprise Architecture Framework, Version 2.0* (September 2008).

⁵² Office of the Program Manager, Information Sharing Environment, *ISE Profile and Architecture Implementation Strategy, Version 2.0* (June 2009).

⁵³ A segment architecture represents a portion of the overall enterprise that can be established as a separate initiative under the overall enterprise architecture.

⁵⁴ The *Federal Segment Architecture Methodology* provides a step-by-step guide for developing segment architectures. See Chief Information Officers Council, Federal Segment Architecture Working Group and Office of Management and Budget, *Federal Segment Architecture Methodology*.

Reporting evaluation environment segment architecture, which is intended to assess selected architectural concepts supporting the business processes, procedures, and policies associated with a nationwide Suspicious Activity Reporting capability, among other things. In addition, as described subsequently in this report, three ISE agencies have developed information sharing segment architectures, which are intended to identify common ISE services, standards, and other ISE tools to allow for opportunities to reuse and leverage services among ISE departments and agencies.

Although the ISE architectural guidance and products provide some information to guide information sharing activities at the five key ISE implementing agencies, they do not fully describe the ISE's current and future environment for business processes, data and information, applications and services, technology, and security consistent with relevant guidance. For example, the EAF identifies 24 current ISE business processes and describes activities and information flows for 3 current business processes.⁵⁵ However, it does not describe business activities and information flows for the remaining 21 current business processes, such as the business process that supports responding to a terrorism-related threat. These information flows are important for identifying specific terrorism data needed to be shared among the ISE business processes and establishing mutually understood data definitions and structures to facilitate data integration across the ISE. Without such common definitions and structures, ISE agencies risk needing to invest significant time and resources to interpret and restructure data received from multiple systems supporting different ISE business processes.

Moreover, the ISE EAF describes some aspects of the future technology environment, such as a set of technical standards that has been identified for use in planning, implementing, and deploying ISE information technology infrastructure, but it does not describe the ISE's current

⁵⁵ According to the ISE EAF, the ISE mission business processes are Suspicious Activity Reporting; Alerts, Warnings, and Notifications; Identification and Screening; Information Requirements and Roles; Analysis; Operations; Policy and Decision Making, Response, and Protection. The service business processes are Information Protection/Assurance, Access, Discovery and Search, Dissemination, Collaboration, Manipulation and Storage, and Electronic Directory Services. The enabling business processes are Issuances, Information Sharing Agreements, Business Process and Performance Management, Training/Cultural Change, Security Framework, Standards and Architecture, Privacy and Civil Liberties Protection, and ISE Governance and Management.

technology environment (e.g., the existing databases and communications networks that support the Alerts, Warnings, and Notifications business process). In addition, an ISE enterprise sequencing plan that describes the interdependent activities to be undertaken by the Program Manager and ISE agencies to incrementally achieve the target ISE does not exist. As a result, ISE agencies and the Program Manager risk not synchronizing or integrating their interdependent ISE activities to inform timely initiation of ISE projects or development of ISE policies and procedures. Appendix III provides a detailed analysis and descriptions of the ISE architectural content reflected in the EAF and associated architectural documents.

If managed properly, an EA program can help simplify, streamline, and clarify the interdependencies and relationships among an enterprise's diverse mission and mission-support operations and information needs, including its associated information technology environment. However, the Office of the Program Manager's approach to managing ISE architecture-related activities does not fully satisfy the core elements described in our EAMMF for establishing institutional commitment and creating the EA management foundation. Of the 13 core elements spanning these two stages that we reviewed, 1 was fully satisfied, 9 were partially satisfied, and 3 were not satisfied. (See app. IV for a detailed description of each core element and our analysis of the extent to which each has been satisfied.) For example, in consultation with the ISA IPC, proactive steps have been taken to address EA-related cultural barriers, such as parochialism and cultural resistance among ISE agencies. However, an EA program management plan that, among other things, reflects ISE EA program work activities, events, and time frames and defines accountability mechanisms does not exist. As a result, ISE agencies risk not budgeting and allocating adequate resources for ISE work activities, and risk delaying the start or completion of their ISE work activities because of a lack of information about the activities and events associated with the ISE EA program. Regardless of the architectural approach used for the ISE, establishing the EA management foundation is important for guiding the development of ISE architecture products to effectively support ISE implementation efforts.

Finally, agency-specific information sharing segment architectures, which according to ISE guidance are to be developed to identify common ISE services, standards, and other ISE tools to allow for opportunities to reuse

and leverage services among ISE departments and agencies, have not been fully defined.⁵⁶ According to the Program Manager's July 2010 annual report to Congress, ODNI and State have not developed such segment architectures. In its technical comments on a draft of this report, ODNI acknowledged that it does not have an information sharing segment architecture, and is working to make data sharable through Intelligence Community policies. For example, Intelligence Community Directive 501 states that all information collected and analysis produced by a member of the intelligence community shall be made available for automated discovery by authorized Intelligence Community personnel, consistent with applicable law and in a manner that protects fully the privacy rights and civil liberties of all U.S. persons.⁵⁷ Also according to the Program Manager's July 2010 annual report to Congress, DOJ, DHS, and DOD have taken steps to develop their respective segment architectures. However, the DOJ, DHS, and DOD information sharing segment architectures are all missing important content. For example, none of these three departments has fully defined the needed business and information requirements. (The extent to which these three departments have developed their information sharing segment architectures is described in app. V.) As a result, there may be an insufficient basis for identifying opportunities to avoid duplication of effort and launch initiatives to establish and implement common, reusable, and interoperable solutions and services across the ISE to achieve cost savings.

The ISE EAF is intended to establish a strategic road map that enables ISE departments and agencies to further develop their respective EAs in order to implement information sharing capabilities. However, as we have previously reported, high-level EA frameworks and guidance, such as OMB's federal EA, do not necessarily provide sufficient content for guiding the implementation of systems.⁵⁸ The ISE EAF and associated architectural documentation also do not (1) provide sufficient architectural

⁵⁶ Each ISE member in the federal government is to develop an information sharing segment architecture that addresses ISE EAF and PAIS guidance as it seeks to connect to the ISE.

⁵⁷ The term "U.S. person" encompasses U.S. citizens and aliens lawfully admitted for permanent residence in the United States (as defined at 8 U.S.C. § 1101(a)(20)). See 50 U.S.C. § 1801(i).

⁵⁸ GAO, *Information Technology: The Federal Enterprise Architecture and Agencies' Enterprise Architectures Are Still Maturing*, [GAO-04-798T](#) (Washington, D.C.: May 19, 2004).

content (e.g., descriptions of ISE business processes and interagency information exchange requirements) necessary for ISE agencies to develop their information sharing architectures or (2) include an ISE enterprise sequencing plan that would serve as an effective road map for ISE departments and agencies. In addition, officials from the key ISE implementing agencies indicated that the lack of detailed and implementable ISE guidance was one limiting factor in developing agency information sharing segment architectures.⁵⁹ Improved ISE architecture content and an ISE enterprise sequencing plan could enable better planning for the distributed ISE and allow for implementation of ISE capabilities in manageable pieces.

The Program Manager stated that his office and OMB are using a standardized EA framework and method for the ISE to identify critical business processes and interfaces, establish standards for data formats, identity management and credentialing, and exchange protocols for information sharing between enterprises in a manner that permits each department and agency to satisfy ISE requirements while also optimizing its own EAs for its specific missions. The Program Manager added that this approach is based on (1) OMB decisions to establish a standardized EA framework that departments and agencies that own their respective information systems and architectures could use to develop, modify, and integrate those systems into the ISE; (2) the Office of the Program Manager's interpretation of the Intelligence Reform Act; and (3) the Office of the Program Manager's understanding that a full EA must be organization based and tied to budget authority.

Nevertheless, the Intelligence Reform Act calls for the Program Manager to plan for and oversee the implementation of the ISE and to assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE. It further calls for the Program Manager to issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and

⁵⁹ Representatives from two ISE agencies stated that existing ISE architecture guidance is not detailed enough to be implementable, and a representative from one of these two agencies cited this lack of detailed guidance as one factor limiting the agency's ability to develop a detailed information sharing segment architecture. Representatives from another ISE agency stated that the lack of a detailed ISE EA limits the agency's ability to develop its respective information sharing segment architecture. And a representative from a fourth ISE agency stated that an ISE EA would improve the ISE Program Manager's ability to develop the ISE.

operation of the ISE, consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of OMB. In addition, the Chief Information Officers Council has previously reported that a well-defined EA can promote better planning and facilitate management of an extensive, complex environment.⁶⁰ Moreover, as described previously in this report, our EAMMF recognizes that EAs can be developed in a distributed manner and accordingly does not prescribe a specific approach by which organizations should develop needed EA content. By not ensuring that an improved EA management foundation for the ISE exists, the federal government, as a whole, is not well positioned to realize the significant benefits that well-defined ISE EA guidance and products can provide. Such benefits include better planning for ISE implementation; improved decision making regarding capability enhancement and resource allocation across the ISE enterprise; increased collaboration on interdependent ISE work activities; and effective sharing of critical terrorism information among appropriate ISE agencies and state, local, and tribal governments and private sector entities.

Conclusions

The ISE is to fulfill a critical purpose in a time when acts of terrorism on U.S. soil have recently been attempted or planned. The Program Manager and key agencies have taken actions to define and implement the ISE, such as developing a framework to advance an initial set of goals, activities, and metrics. However, they also recognize that these actions do not yet go far enough to define and implement a fully functioning ISE and that there is more work to do. In addition, our work has identified actions that are needed after the end state vision for the ISE is defined, such as ensuring that all relevant information sharing initiatives across the five communities are fully leveraged by the ISE, consistent with the Intelligence Reform Act. This could help to ensure that all critical information with a possible nexus to terrorism is being shared as needed, and that relevant agency initiatives are considered to determine how they could be leveraged by the ISE for the benefit of all stakeholders, thereby helping to improve information sharing governmentwide. Also, to the extent possible, defining incremental costs necessary to implement the ISE, consistent with the Intelligence Reform

⁶⁰ Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0.

Act, could help decision makers plan for and prioritize future investments. Further, while the Program Manager has taken steps to measure and demonstrate results of ISE efforts, additional actions are needed to address our prior recommendations to ensure that the ISE is on a measurable track to success and to show the extent to which the ISE has been implemented, what work remains, and milestones for completing remaining work.

The Program Manager and ISE agencies have developed architecture guidance and products—such as the EAF—to assist in implementing the ISE, but crucial work remains. The guidance and products provide some foundational information about the ISE, but they do not fully define the suite of ISE architecture products that describe the ISE current and future operational and technical environment to support ISE implementation. Further, ISE EA management practices do not fully address the core elements described in our EAMMF, such as establishing an EA program management plan that, among other things, reflects ISE EA program work activities, events, and time frames and defines accountability mechanisms. Moreover, it is unclear when, how, and by whom these core elements will be satisfied and missing architecture content—such as business activities and information flows, the ISE technology environment, and an enterprise sequencing plan—will be developed. Establishing an improved EA management foundation, including well-defined EA guidance for the ISE, would better position the government to realize significant benefits, such as better planning for implementation, improved decision making, and ultimately more effective sharing of critical terrorism-related information among all ISE agencies.

Recommendations for Executive Action

To help ensure effective implementation of the ISE, we recommend that the Program Manager, with full participation from relevant stakeholders, take the following three actions.

To support future progress in developing and implementing the ISE, we recommend that after the end state is defined, the Program Manager

- in consultation with the ISA IPC and key ISE agencies, determine to what extent relevant agency initiatives across all five communities could be better leveraged by the ISE so that their benefits can be realized governmentwide and
- in coordination with the ISA IPC and OMB, task the key ISE agencies to define, to the extent possible, the incremental costs needed to help

ensure successful implementation of the ISE and prioritize investments.

To better define ISE EA guidance and effectively manage EA activities to support ISE implementation efforts, we recommend that the Program Manager, in consultation with the ISA IPC and key ISE agencies, establish an ISE EA program management plan that (1) reflects ISE EA program work activities, events, and time frames for improving ISE EA management practices and addressing missing architecture content and (2) defines accountability mechanisms to help ensure that this program management plan is implemented.

Agency Comments and Our Evaluation

We provided a draft of this report for comment to the Program Manager for the ISE, OMB, DHS, DOJ, State, DOD, and ODNI. Based on subsequent discussions with officials from the Office of the Program Manager, we revised portions of the draft that discuss the ISE EA and the related recommendation to clarify that our focus is primarily on architectural management practices and that various approaches can be used for structuring an EA. We received written responses from the Program Manager and DHS, which are summarized below and reprinted in appendix VI and appendix VII, respectively. Also, on June 17, 2011, the Federal Chief Enterprise Architect and other OMB officials provided oral comments. The Program Manager and Federal Chief Enterprise Architect generally agreed with the three recommendations in this report, while DHS did not address them. The Program Manager, DHS, DOJ, and ODNI provided technical comments, which we have incorporated in this report where appropriate. State and DOD informed us that they had no comments.

Program Manager's Comments

The Program Manager's written comments did not specifically mention whether he agreed with the three recommendations in this report, but the Office of the Program Manager subsequently confirmed via e-mail on July 7, 2011, that the Program Manager generally agreed with all of them, with elaboration as follows.

Leveraging Agency Initiatives

The Program Manager generally agreed with the first recommendation related to the need to determine to what extent relevant agency initiatives across all five communities are being leveraged by the ISE. He noted that the Program Manager and the ISA IPC have already leveraged a great number of initiatives that support the realization of the ISE and that they

will continue to identify and leverage agency initiatives to improve information sharing. The Program Manager provided numerous examples of activities that he said have been leveraged by the ISE and referred us to the annual reports to Congress for more examples. We recognize that the examples provided illustrate agency initiatives to share information and several of them are discussed in this report. In general, however, the Program Manger has not demonstrated how these initiatives are being leveraged by the ISE for the benefit of all stakeholders and to help improve information sharing governmentwide. The Program Manager expects the updated *National Strategy for Information Sharing*—complemented by follow-on implementation policy, programmatic and budgetary guidance, and performance metrics—to address this recommendation. The updated strategy and follow-on guidance and metrics could address the intent of the recommendation if they appropriately discuss how initiatives are being leveraged by the ISE.

Defining Incremental Costs

The Program Manager generally agreed with the second recommendation related to the need to define incremental costs for the ISE. However, he noted that OMB has the role of providing programmatic guidance and collecting budgetary requirements, and ensuring that they are integrated into the budget for each federal department and agency. The Program Manager also said that it is critical to note that federal departments and agencies own, plan for, and manage their programs, systems, and architectures, while the Office of the Program Manager provides the integrating guidance through the ISA IPC. Further, he noted that the individual departments and agencies are responsible for identifying costs over and above their program baselines to extend the benefits of information sharing throughout the ISE. We recognize that OMB and agencies play key roles in defining incremental costs for the ISE. Nevertheless, the Program Manager is responsible for leading and coordinating these efforts, as envisioned by the Intelligence Reform Act. Thus, we believe that the Program Manager is the appropriate party to task key ISE agencies to define, to the extent possible, the incremental costs needed to help ensure successful implementation of the ISE. The Program Manager expects the updated *National Strategy for Information Sharing* and other activities—including programmatic and budgetary guidance—to address this recommendation. The updated strategy and follow-on guidance could address the intent of the recommendation if they support defining incremental costs needed to help ensure successful implementation of the ISE.

Enterprise Architecture

The Program Manager generally agreed with the third recommendation related to the need to more fully define ISE EA plans. He stated that the

ISE needs an integrated plan with an established vision, goals, policy framework, performance management framework, and guidelines. From a planning perspective, the Program Manager noted that the *National Strategy on Information Sharing*—to be updated in the near future—followed by an integrated suite of implementation guidance and practices (e.g., the ISE EAF and the PAIS) provide the tools to effectively manage the ISE. He added that through these and other documents, the Office of the Program Manager will establish the vision, a program management plan, and an executable road map for the ISE. Further, he noted that the office will work with ISE departments and agencies to identify and prioritize their projects in support of the ISE. These actions could address the intent of the recommendation if the strategy and suite of implementation guidance and practices establish an ISE EA program management plan that (1) reflects ISE EA program work activities, events, and time frames for improving ISE EA management practices and addressing missing architecture content and (2) defines accountability mechanisms to help ensure that this program management plan is implemented.

The Program Manager also provided comments indicating that much of this report treats the ISE as a centrally designed and defined information system enterprise and stated that our analysis looks for the tools and processes applicable to such an enterprise. This report and the EAMMF that comprises the basis for much of our analysis recognize that various approaches for structuring an EA exist and can be applied to the extent that they are relevant and appropriate for a given enterprise. As stated in this report and our EAMMF, these approaches generally provide for breaking down an enterprise into its logical parts and allowing various components of an enterprise (e.g., ISE mission partners) to develop their respective parts of the EA in relation to enterprisewide needs and the inherent relationships and dependencies that exist among the parts. For example, this report acknowledges agency-developed information sharing segment architectures—which can represent a portion of an ISE EA—and states that improved ISE architecture content and an ISE enterprise sequencing plan could enable better planning for the distributed ISE.

In addition, the Program Manager stated that he consulted with the key ISE agencies and they agreed that they do not need or want the Program Manager to establish additional ISE EA guidance or an ISE EA. As we previously noted, various approaches can be used for structuring an EA. However, our work showed that agency information sharing architectures were either not developed or incomplete, and that pertinent officials from ISE agencies cited the lack of detailed and implementable ISE guidance

as one factor limiting their efforts to develop agency information sharing architectures. Thus, we believe that an ISE EA program management plan is needed that (1) reflects ISE EA program work activities, events, and time frames for improving ISE EA management practices and addressing missing architecture content and (2) defines accountability mechanisms to help ensure that this program management plan is implemented.

Agency Roles and Responsibilities

In addition to providing comments on each of the three recommendations, the Program Manager noted that the draft report did not fully address the roles and responsibilities of OMB and the departments and agencies that support the ISE, and that recognizing the key roles played by these entities is pivotal to assessing progress in the ISE. He explained that OMB plays a key role in the planning, budgeting, and oversight of the federal agencies and their contributions to the ISE. He also noted that it is primarily through the partnership between OMB and the Office of the Program Manager that program direction, funding, and performance measurement can be effectively achieved. He added that departments and agencies (1) are responsible for developing, deploying, modifying, and maintaining their respective information system investments and associated EAs and (2) play an active role in determining the policies, priorities, and direction of the ISE—originally through the Information Sharing Council—and are now an integral part of the ISA IPC. Further, the Program Manager noted that the information they share and the tools used to share it are by their nature a part of the ISE, regardless of whether the process is identified by the Program Manager. We recognize that OMB and agencies play important roles in defining and building the ISE. Nevertheless, the Program Manager is responsible for leading and coordinating these efforts, in accordance with the Intelligence Reform Act. Thus, we directed the recommendations to him, in consultation with the ISA IPC, key ISE agencies, and OMB as appropriate.

Other Agencies' Comments

In oral comments provided on June 17, 2011, the Federal Chief Enterprise Architect and other OMB officials generally agreed with all three recommendations in this report. Regarding the first recommendation to ensure that agency initiatives are leveraged, the Federal Chief Enterprise Architect noted that all five ISE primary areas of focus (homeland security, law enforcement, foreign affairs, defense, and intelligence) are important and that the Program Manager should continue to ensure effective coordination of these communities. He added that such coordination should occur in consultation with OMB and appropriate agencies at the federal, state, local, and tribal levels. Regarding the

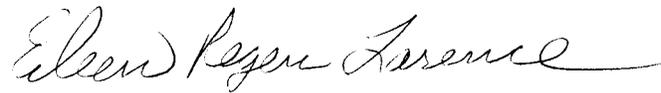
second recommendation to identify incremental costs, the Federal Chief Enterprise Architect noted that the Program Manager should work in collaboration with OMB and federal agencies to identify investments that are related to the ISE, and ensure that waste and duplication are not occurring and that the execution of the program is consistent with legal mandates and administration policies and priorities. Regarding the third recommendation to more fully define ISE EA plans, the Federal Chief Enterprise Architect agreed that our EAMMF was appropriate for evaluating the ISE EA and that the Office of the Program Manager should issue an EA program management plan that contains milestones, time frames, and accountability mechanisms. He noted that the Program Manager and ISE agencies each have a role in developing ISE architecture products.

In its written comments, DHS noted that the department remains committed to continuing its work with the Program Manager and relevant stakeholders to further define and implement a fully functioning ISE. DHS added that the department is engaged with the Program Manager on a number of key initiatives at the ISA IPC to ensure the realization of information sharing benefits governmentwide.

We are sending copies of this report to the Program Manager for the Information Sharing Environment; the Director of National Intelligence; the Director of the Office of Management and Budget; the Secretaries of the Departments of Defense, Homeland Security, Justice, and State; and appropriate congressional committees. This report also is available at no charge on the GAO Web site at <http://www.gao.gov>.

Should you or your staff have any questions about this report, please contact Eileen R. Larence at (202) 512-6510 or larencee@gao.gov or David A. Powner at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be

found on the last page of this report. Key contributors to this report are acknowledged in appendix VIII.



Eileen R. Larence
Director
Homeland Security and Justice Issues



David A. Powner
Director
Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

Our reporting objectives were to review to what extent the Program Manager for the Information Sharing Environment (ISE) and key stakeholder agencies have (1) made progress in developing and implementing the ISE, and what work remains, and (2) defined an enterprise architecture (EA) to support ISE implementation efforts.¹ The stakeholder agencies we reviewed are the five agencies that the Program Manager identified as critical to developing and implementing the ISE—the Departments of Homeland Security (DHS), Justice (DOJ), State (State), and Defense (DOD) as well as the Office of the Director of National Intelligence (ODNI). These agencies represent five information sharing communities identified that collect the homeland security, law enforcement, foreign affairs, defense, and intelligence information deemed critical for sharing in order to provide for homeland security.²

To determine the extent to which the Program Manager and stakeholder agencies have made progress in developing and implementing the ISE, we reviewed key statutes and policies, including the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and the Implementing Recommendations of the 9/11 Commission Act of 2007. We also reviewed our prior reports and best practices identifying effective program management, federal coordination, and cost estimation.³

¹ An EA can be viewed as a reference or “blueprint” for achieving strategic business goals and outcomes, including maximizing information sharing within and across organization boundaries. A well-defined EA provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., homeland security) by documenting the entity’s current operational and technological environment and its target environment, as well as a plan for transitioning from the current to the target environment.

² In total, there are 15 ISE departments and agencies. In addition to the five key agencies (DHS, DOJ, State, DOD, and ODNI), the other 10 are the Central Intelligence Agency, the Department of Commerce, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Department of Transportation, the Department of the Treasury, the Federal Bureau of Investigation, the Joint Chiefs of Staff, and the National Counterterrorism Center.

³ See, for example, GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); Project Management Institute, *The Standard for Program Management* © (2006); GAO, *Determining Performance and Accountability Challenges and High Risks*, [GAO-01-159SP](#) (Washington, D.C.: November 2000); GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005); and GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009).

Through our review of these laws, guidance, and reports, we identified standards and best practices for program and project management and used them to inform our assessment of efforts to develop and implement the ISE and related efforts. We used semistructured interviews to gather information from the key agencies and facilitate analysis of their perspectives on the development of and remaining challenges impeding implementation of the ISE. We also used interviews to obtain information from these agencies on the status of key activities the Program Manager identified as accomplishments in the 2009 and 2010 ISE annual reports to Congress, among other things.⁴ In addition, we reviewed and analyzed agency documentation on guidance and plans and conducted interviews with agency officials to assess actions taken by the Program Manager to address recommendations in our 2008 report related to defining the purpose and scope of the ISE and the results to be achieved.

To determine to what extent the Program Manager for the ISE and key stakeholder agencies have defined an EA to support ISE implementation efforts, we examined the extent to which (1) key current, or “as-is,” and future, or “to-be,” EA content and a plan for transitioning from the current to the future environment have been established; (2) the Office of the Program Manager has established a structure for effectively managing ISE architecture development and implementation; and (3) key federal agencies have defined their information sharing segment architectures (ISSA) to support ISE implementation.

To determine the extent to which key current and future EA content, and a plan for transitioning from the current to the future environment has been established, we compared ISE architecture guidance, such as the ISE Enterprise Architecture Framework (EAF) and associated

⁴ See Office of the Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment* (June 2009), and *Annual Report to the Congress on the Information Sharing Environment* (July 2010). See also U.S.C. § 485(h) (requiring the submission of annual performance management reports on the state of the ISE and information sharing across the federal government).

documents,⁵ to relevant EA content guidance.⁶ We also interviewed officials from the Office of the Program Manager, including the Program Manager and the Executive for Programs and Technology, as well as officials from the key federal agencies, to determine, among other things, their perspectives on ISE architecture content. In addition, we met with Office of the Program Manager officials to discuss variances between ISE EA content reflected in the ISE EAF and associated documents and EA content expectations established in relevant federal guidance.

To determine the extent to which the Office of the Program Manager has established a structure for effectively managing ISE architecture development and implementation, we used our Enterprise Architecture Management Maturity Framework (EAMMF),⁷ and determined the extent to which the Office of the Program Manager has satisfied key elements associated with providing institutional leadership and foundational management capabilities. To make this determination, we reviewed relevant ISE documentation, including Executive Order 13,388 (October 25, 2005); the December 16, 2005, presidential memorandum regarding Guidelines and Requirements in Support of the Information Sharing Environment; the Intelligence Reform Act; Program Manager guidance; and Chief Architects Roundtable and Common Information Sharing Standards working groups' meeting minutes. We also interviewed officials from the Office of the Program Manager and compared documentation

⁵ See, for example, Office of the Program Manager, Information Sharing Environment, *Information Sharing Environment: Annual Report to the Congress* (June 2009); *ISE Profile and Architecture Implementation Strategy*, Version 2.0 (June 2009); *ISE Enterprise Architecture Framework*, Version 2.0 (September 2008); *ISE Functional Standard Suspicious Activity Reporting*, Version 1.5; and *ISE Guidance, Technical Standards – Core Transport*, Version 1.0.

⁶ See, for example, GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C.: August 2010); Office of Management and Budget, *FEA Consolidated Reference Model Document*, Version 2.3 (October 2007); Chief Information Officers Council, Federal Enterprise Architecture Program Management Office, *The Federal Enterprise Architecture Security and Privacy Profile*, Version 2.0 (June 1, 2006); Federal Enterprise Architecture Program, *The Data Reference Model*, Version 2.0 (Nov. 17, 2005); Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); Office of Management and Budget Circular A-130, Revised (Transmittal Memorandum No. 4), Memorandum for Heads of Executive Departments and Agencies on Management of Federal Information Resources; and Chief Information Officers Council, *Federal Enterprise Architecture Framework*, Version 1.1 (September 1999).

⁷ [GAO-10-846G](#).

collected and information provided during interviews to determine the extent to which the office and the Information Sharing and Access Interagency Policy Committee addressed EAMMF elements associated with establishing institutional commitment and direction and creating the management foundation for EA development and use. We did not evaluate the extent to which the ISE architecture program had adequate staff and budget resources because of the lack of a stand-alone budget for the ISE program and the classified nature of the ODNI budget.

To determine the extent to which key federal agencies have defined their ISSAs to support ISE implementation, we determined the extent to which agency-developed ISSAs have addressed ISE architecture guidance established by the Office of the Program Manager. Specifically, we determined key ISSA development steps defined in the Program Manager's *Profile and Architecture Implementation Strategy* that are consistent with best practices documented in the *Federal Segment Architecture Methodology*.⁸ We then reviewed the agency-developed ISSAs and relevant supporting documentation, such as information sharing strategies and information sharing implementation plans, against these key ISSA development steps. We also interviewed officials from DOD (the Office of the Assistant Secretary for Defense, Networks and Information Integration/DOD Chief Information Officer (CIO)), DHS (Office of the CIO), DOJ (Justice Management Division/Office of the CIO), and State (Office of Management Policy, Rightsizing, and Innovation) to understand the reasons why the agency-developed ISSAs have yet to fully address the key ISSA development steps.

We conducted this performance audit from October 2009 through July 2011 in accordance with generally accepted government auditing standards.⁹ 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

⁸ Federal Segment Architecture Working Group and Office of Management and Budget, *Federal Segment Architecture Methodology* (December 2008).

⁹ This time frame reflects the fact that in June 2010, the President appointed the current Program Manager, and we needed time to assess his plans for moving forward with development of the ISE and to obtain perspectives from the five key ISE agencies on this change in leadership and on his plans. In the interim, we reported on preliminary results related to the overall review and the current Program Manager's plans in our February 2011 high-risk update on the federal government's sharing of terrorism-related information. See [GAO-11-278](#).

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

Appendix II: ISE Framework Goals and Subgoal Activities

To better define and manage ISE implementation, the Program Manager adopted the ISE framework to guide development of the ISE going forward. Specifically, the framework identified four goals and 14 specific subgoals or activities agencies were to pursue. The goals and subgoals follow.

Goal 1: Create a Culture of Sharing

Subgoal 1.1: Information sharing is exhibited across departments and agencies as a routine part of doing business and recognized as an imperative to success.

Subgoal 1.2: All personnel charged with sharing terrorism-related information are trained to carry out information sharing responsibilities.

Subgoal 1.3: Employees are routinely recognized and rewarded for effective information sharing, as well as expertise and competency development.

Goal 2: Reduce Barriers to Sharing

Subgoal 2.1: Federal departments and agencies practice security reciprocity among federal, state, local, and private sector entities, including people, facilities, and systems.

Subgoal 2.2: Consistent marking and handling of controlled unclassified information is practiced across the U.S. government; practices are also adopted by state, local, tribal, and private sector entities.

Subgoal 2.3: ISE participants build trusted distributed infrastructure for sharing information with all other participants, and are able to leverage repeatable processes from each others' architecture programs to maximize availability of common ISE shared services.

Subgoal 2.4: ISE departments and agencies; state, local, and tribal governments; and the private sector protect privacy in a consistent manner.

Goal 3: Improve Sharing Practices with Federal, State, Local, Tribal, and Foreign Partners

Subgoal 3.1: All federal, state, local, tribal, and law enforcement entities operating domestically participate in a standardized, integrated approach

to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity information.

Subgoal 3.2: A national, integrated network of state and major urban area fusion centers that enables federal, state, local, tribal, and private sector organizations to gather, document, process, analyze, and share relevant information in order to protect our communities.

Subgoal 3.3: Federal agencies produce, share, and disseminate both time-sensitive and strategic information and intelligence products that meet state, local, tribal, and private sector needs.

Subgoal 3.4: Federal departments and agencies have implemented appropriate policies and processes to coordinate and facilitate the sharing of information with foreign governments and allies.

Goal 4: Institutionalize Sharing

Subgoal 4.1: Integrated performance and investment processes monitor progress toward performance goals and successfully use investments to support activities that maintain or enhance information sharing.

Subgoal 4.2: ISE participants sustain their investments in information systems that support a trusted, distributed infrastructure for sharing information.

Subgoal 4.3: ISE participants use common practices and policies for producing, handling, and using information.

Appendix III: Analysis of ISE Architecture Content

According to relevant guidance, an enterprise architecture (EA) should describe architectural views of the business processes, data, applications and services, technology, and security for the enterprise's current and future environments.¹ An EA should also include a sequencing plan for transitioning from the current environment to the future environment. Table 1 describes the extent to which the Information Sharing Environment (ISE) architecture documents address such relevant EA guidance.

Table 1: ISE Architecture's Satisfaction of Relevant EA Guidance

Content area and description	Analysis of ISE architecture framework content
Business: The business view should include, among other things, business process descriptions, including the business activities/tasks performed and the information flows among activities/tasks.	The ISE Enterprise Architecture Framework (EAF) identifies three types of business processes: (1) mission processes, (2) service processes, and (3) enabling processes. In addition, it identifies 24 distinct current business processes and associates each business process with one of the three process types. ^a Further, it includes business activities/tasks and information flows associated with 3 current business processes (i.e., Suspicious Activity Reporting (SAR); Alerts, Warnings, and Notifications (AWN); and Identification and Screening). However, the EAF and associated documentation provided by the Program Manager and ISE agencies do not include business activities/tasks and information flows for the remaining 21 current business processes (e.g., Response). In addition, the EAF does not identify mission processes that are cited in the 2010 ISE annual report to Congress, such as the Law Enforcement Information Sharing mission process or the Sharing with International Partners mission process. Moreover, neither the EAF nor the Profile and Architecture Implementation Strategy (PAIS) identifies or describes any future ISE business processes.

¹ See, for example, [GAO-10-846G](#); Chief Information Officers Council, Federal Enterprise Architecture Program Management Office, *The Federal Enterprise Architecture Security and Privacy Profile*, Version 2.0 (June 1, 2006); Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001); and Office of Management and Budget Circular A-130, Revised (Transmittal Memorandum No. 4), Memorandum for Heads of Executive Departments and Agencies on Management of Federal Information Resources.

Content area and description	Analysis of ISE architecture framework content
<p>Data: The data view should describe the data needed to support the business needs (i.e., data context), the meaning and structure of the data (i.e., data description), how the data are to be made available (i.e., data sharing), and data management practices.</p>	<p>While the ISE EAF and associated documents address the data context and data description of the current SAR mission process (e.g., hair color text and hair color code), these documents do not provide data descriptions and context for the other current ISE mission processes (e.g., AWN) or address data descriptions and data context of terrorism information to be exchanged among the ISE business processes. In addition, while the ISE EAF describes capabilities (e.g., query) to search for current terrorism data, it does not describe the current practices for managing terrorism data (e.g., managing the reliability of terrorism data from multiple sources) and related issues (e.g., semantics inconsistency and information overloads). With respect to the future data environment, the EAF only cites a data repository concept (i.e., shared spaces) for making terrorism-related information accessible to ISE participants; however, neither the ISE EAF nor associated documents provided by the Office of the Program Manager and ISE agencies include data descriptions and the data context for information to be used by future ISE mission processes because such future business processes have not yet been defined. In addition, these documents do not specify data management best practices (e.g., data quality management) for the future environment.</p>
<p>Applications and services: The applications and services view should include descriptions of enterprise application systems and service components and the interfaces required to access them, as well as the relationships among the applications and services and the business processes they support.</p>	<p>The ISE EAF states that numerous current systems in the federal government contain useful information that can be leveraged for information sharing. According to the Office of the Program Manager for the ISE, Executive for Programs and Technology, the Office of Management and Budget has collected this information from agencies, and the Office of the Program Manager has access to it. However, the ISE EAF and associated documentation provided by the Program Manager and key ISE agencies do not include a comprehensive list of these current ISE systems. In addition, the EAF does not include the relationships between these current systems and the ISE business processes that they support. With respect to the future environment, the EAF identifies future types of core services (e.g., discovery, security, mediation, messaging, enterprise service management, storage, and collaboration) and portal services (e.g., user interface, portal hosting, publish/subscribe, user assistance, and collaboration), which are intended to support terrorism-related information sharing among ISE agencies. It also maps the relationships of some of these core services to ISE mission processes. However, the EAF and associated documentation do not describe future application systems and services that are critical to each ISE mission process. For example, the ISE EAF does not identify future mission-critical application systems and services for the identification and screening mission process.</p>
<p>Technology: The technology view should include descriptions of critical information technology (IT) infrastructure systems that are to support the enterprise and the technical standards and technologies that are to be used in implementing enterprise application systems and services.</p>	<p>The ISE EAF and associated documentation do not include a complete description of the current technology environment. For example, these documents do not describe current IT infrastructure system assets that currently support each of the ISE business processes (e.g., the existing databases and communication networks that support the AWN business process). However, the EAF does describe aspects of the future technology environment. For example, a set of technical standards (i.e., ISE-G-107^b) has been identified for use in planning, implementing, and deploying ISE IT infrastructure. In addition, the EAF identifies technologies (e.g., Enterprise Service Bus) that can be used for the ISE IT infrastructure, and it cites a set of technical standards (e.g., extensible hypertext markup language) for ISE participants to consider in planning and implementing the previously mentioned ISE shared spaces. However, the EAF and associated documentation do not define all key technical standards. For example, while the EAF states that the Common Information Sharing Standards Universal Core is intended to be the foundation for ISE information exchanges, these standards have yet to be fully defined. In addition, future ISE IT infrastructure is not identified and described. For example, key characteristics of the ISE future network infrastructure, including a network topology (e.g., a token ring configuration) that would depict how the ISE agencies' shared spaces would interconnect, are not described.</p>

**Appendix III: Analysis of ISE Architecture
Content**

Content area and description	Analysis of ISE architecture framework content
<p>Security: The security view should include descriptions of enterprise-level security requirements, security controls and services, security standards (e.g., access control protocol), and security management processes (e.g., risk management and audit and accountability).</p>	<p>The ISE EAF and associated documents do not fully describe the current ISE security environment. For example, while the PAIS describes security requirements for developing ISE shared spaces (e.g., each ISE shared space front-end Web server should validate the identities of external ISE participants requesting access to a local ISE shared space database), it does not specifically describe the existing security controls (e.g., network access control software) that are to be leveraged to achieve information confidentiality (e.g., appropriate disclosure), integrity (e.g., protection against improper or accidental modification), and availability (e.g., timely and reliable access). Further, while the EAF addresses aspects of security management processes by describing the ISE risk management framework for achieving trustworthiness for ISE information systems and by describing the Identity and Access Management framework for achieving identity and information access portability across the ISE, the EAF and associated documentation have not defined all key ISE information assurance standards and associated implementation guidelines, such as standards for segregating data into different security domains (e.g., Top Secret, Secret, and Sensitive but Unclassified/Controlled Unclassified Information). Further, the EAF and associated documentation do not link security requirements to each ISE mission process. For example, the documents do not describe specific, measurable security requirements (e.g., security audit, cryptography, etc.) for the Identification and Screening mission process.</p>
<p>Sequencing plan: A sequencing plan should provide a solid basis upon which to build and should reflect, among other things, capabilities that support business processes; governmentwide and agency-specific investments that provide such capabilities, notional dependencies if any among these investments, expectations about investment timelines, costs, and benefits; and emerging and available technological opportunities (e.g., cloud computing).</p>	<p>An ISE EA enterprise sequencing plan does not exist.</p>

Source: GAO analysis of ISE documents and interviews.

^aAccording to the ISE EAF, the ISE mission business processes are SAR, AWN, Identification and Screening, Information Requirements and Roles, Analysis, Operations, Policy and Decision Making, Response, and Protection. The service business processes are Information Protection/Assurance, Access, Discovery and Search, Dissemination, Collaboration, Manipulation and Storage, and Electronic Directory Services. The enabling business processes are Issuances, Information Sharing Agreements, Business Process and Performance Management, Training/Cultural Change, Security Framework, Standards and Architecture, Privacy and Civil Liberties Protection, and ISE Governance and Management.

^bISE-G-107, or *Information Sharing Environment Guidance, Technical Standard Core Transport*, Version 1.0, was issued by the Office of the Program Manager to describe the voluntary standards to be followed by the ISE implementing agencies in planning, implementing, and deploying ISE IT infrastructure, and by ISE participant agencies in aligning these technical standards with existing IT standards for interfaces between their ISE shared spaces and the ISE core.

Appendix IV: ISE’s Satisfaction of Selected EA Institutional Leadership and Management Controls

Table 2 describes the Information Sharing Environment’s (ISE) satisfaction of selected core elements in stages 1 and 2 of our Enterprise Architecture Management Maturity Framework (EAMMF).

Table 2: ISE’s Satisfaction of Selected EAMMF Core Elements

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>Written and approved organization policy exists for enterprise architecture (EA) development, maintenance, and use. An organization should have a documented policy, approved by the organization head, to institutionalize the architecture’s importance, role, and relationship to other corporate management disciplines. Among other things, the policy should</p> <p>(1) define the EA as consisting of the current and target architecture, as well as the transition plan for migrating from the current to the target architecture;</p> <p>(2) provide for EA development, maintenance, and use;</p> <p>(3) identify the major players associated with EA development, maintenance, and use, including the chief architect, program office(s), executive committee, investment review board(s), and chief information officer (CIO);</p> <p>(4) provide for developing a performance and accountability framework that identifies each player’s roles, responsibilities, and relationships and describes the results and outcomes for which each player is responsible and accountable; and</p> <p>(5) acknowledge the interdependencies and relationships among the EA program and other related institutional management disciplines, such as strategic planning, human capital management, information security management, privacy, records management, and capital planning and investment control.</p>	<p>Partially satisfied.</p> <p>(1) The December 16, 2005, presidential memorandum regarding Guidelines and Requirements in Support of the Information Sharing Environment states that the ISE will be developed leveraging, among other things, existing architectures. In addition, the memorandum that accompanies the most recent version of the ISE Enterprise Architecture Framework (EAF) states that the framework provides a strategic roadmap to enable long-term business and technology standardization and information systems planning, investing, and integration. However, neither of these documents explicitly defines an ISE EA as consisting of a current and future architecture, as well as a transition plan for migrating from the current to the target architecture.</p> <p>(2) No policy or guidance, including Executive Order 13,388 (October 25, 2005) and the presidential memorandum, explicitly calls for the development, maintenance, and use of an ISE EA.</p> <p>(3) Various policy documents identify key players associated with the ISE. For example, the EAF calls for the five ISE communities (defense, foreign affairs, homeland security, intelligence, and law enforcement) and their respective federal departments as well as state, local, and tribal governments; the private sector; and foreign governments to be responsible for leveraging the EAF to facilitate information sharing. Further, the EAF identifies key ISE member agencies and defines the roles and responsibilities of ISE implementing agencies and ISE participating agencies. In addition, a May 2009 presidential memorandum designated the National Archives and Records Administration as the executive agent responsible for creating and carrying out a governmentwide framework for controlled unclassified information. However, none of these documents explicitly identify the lead entity responsible for the development, maintenance, and use of an ISE EA.</p> <p>(4) The Program Manager for the ISE adopted an ISE performance framework^a in 2009. In addition, the Program Manager’s annual report describes progress in meeting the goals and subgoals outlined by this performance framework. The annual report also provides high-level information (i.e., a yes or no) on each ISE department and agency’s efforts to achieve architecture-related objectives—e.g., integrating information technology (IT) management structures with ISE EA principles—by taking specific actions (e.g., mapping at least one IT investment to their information sharing segment architectures). However, the performance framework does not explicitly identify roles, responsibilities, and relationships or describe the results and outcomes for which each player is responsible and accountable relative to developing an ISE EA.</p> <p>(5) The ISE performance framework includes a subgoal associated with integrating EA and capital planning and investment control. However, the performance framework does not discuss interdependencies and relationships between an ISE EA program and other related institutional management disciplines (e.g., strategic planning).</p>

**Appendix IV: ISE's Satisfaction of Selected EA
Institutional Leadership and Management
Controls**

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>Executive committee representing the enterprise exists and is responsible and accountable for EA. An organization should assign responsibility and accountability for directing, overseeing, and approving the architecture not to just one individual, but to a formally chartered executive committee with active representation from across the enterprise. Establishing enterprisewide responsibility and accountability is important for demonstrating the organization's institutional commitment to EA and for obtaining buy-in from across the organization. Specifically, the committee should</p> <p>(1) be composed of executive-level representatives from each line of business, and these representatives should have the authority to commit resources and enforce decisions within their respective organizational units;</p> <p>(2) include executive representation from other related organizations if the EA extends beyond traditional organizational boundaries (e.g., across multiple departments or agencies); and</p> <p>(3) be chartered by the head of the organization (e.g., the department or agency head) and be responsible for establishing the EA's purpose, goals, strategy, and performance and accountability framework, and for ensuring that EA plans, management processes, products, and results are achieved.</p>	<p>Partially satisfied.</p> <p>(1) The Information Sharing and Access Interagency Policy Committee (ISA IPC), which is composed of executive-level representatives from each ISE member organization, is to assist the Program Manager in carrying out his duties. The committee is co-chaired by the Senior Director for Information Sharing Policy, who serves under the Executive Office of the President, and the ISE Program Manager. To support this committee, the Standards and Architecture sub-IPC and its two working groups (i.e., the Chief Architects Roundtable (CAR) and the Common Information Sharing Standards (CISS)) have assisted in coordinating and facilitating the development of ISE standards and architectures across the ISE agencies. However, these officials also stated that a review is under way that might change this governance structure.</p> <p>(2) According to CAR and CISS working group meeting minutes and agendas as well as officials from participating departments, these groups include representation from ISE member agencies.</p> <p>(3) The ISA IPC replaced the Information Sharing Council established by the Intelligence Reform and Terrorism Prevention Act of 2004. Neither the ISA IPC nor any other entity has explicitly been assigned responsibility and accountability for directing, overseeing, and approving an ISE EA, to include responsibility for establishing the purpose, goals, strategy, and performance and accountability framework for an ISE EA and for ensuring that ISE EA plans, management processes, products, and results are achieved.</p>

Appendix IV: ISE's Satisfaction of Selected EA Institutional Leadership and Management Controls

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>Executive committee is taking proactive steps to address EA cultural barriers. Parochialism and cultural resistance to change are significant barriers to organizations having a mature EA. Accordingly, we have previously reported on the need for sustained executive leadership to overcome these and other barriers. Among other things, this can include</p> <ul style="list-style-type: none"> (1) proactive steps by the executive committee and its members to promote and reward EA-related collaboration across organizational boundaries and (2) committing component organization resources to EA activities, and encouraging the disclosure and adoption of EA shared services. 	<p>Satisfied.</p> <ul style="list-style-type: none"> (1) The ISA IPC, along with its Standards and Architecture sub-IPC and CISS and CAR working groups, has taken steps to address cultural barriers across the ISE. For example, the Program Manager's 2009 and 2010 annual reports identify creating a culture of sharing as an explicit goal and report on department and agency efforts to make progress toward achieving this goal, such as incorporating information sharing into staff performance evaluations. In addition, according to the Office of the Program Manager's Executive for Programs and Technology and our review of associated meeting agendas and minutes, the CISS and CAR working groups provide a forum to facilitate the establishment of a common architectural language and terms and to potentially address cultural barriers. (2) Agendas, meeting minutes, and the participation of officials from participating departments demonstrate that executive leadership at the participating ISE agencies is willing to commit staff resources to ISE architecture and standards related activities.
<p>Chief architect exists.</p> <ul style="list-style-type: none"> (1) An organization should have a chief architect who leads the corporate EA program office and who is responsible for EA development and maintenance and accountable to the executive committee. (2) The chief architect is typically an organization executive whose background and qualifications span both the business and technology sides of the organization. Because the chief architect also typically serves as the EA program manager, this person should be knowledgeable about program management as well as capital planning and investment control, systems engineering, and organization and data modeling. (3) The chief architect (in collaboration with the CIO, executive committee, and the organization head) is instrumental in obtaining organizational buy-in for the EA (including support from the business units) and in securing resources to support architecture management functions, such as risk management, configuration management, and quality assurance. As such, the chief architect acts as the corporate spokesperson and advocate for EA adoption. 	<p>Partially satisfied.</p> <ul style="list-style-type: none"> (1) The ISE Program Manager, who co-chairs the ISA IPC, has been assigned some of the responsibilities expected of an ISE chief architect. For example, the Intelligence Reform Act assigns the Program Manager responsibility for assisting in the development of policies, as appropriate, to foster the development and proper operation of the ISE. It further calls for the Program Manager to issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE, 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. In addition, the Executive for Programs and Technology has supported the Program Manager in guiding and managing existing ISE architecture efforts on a day-to-day basis. However, the currently assigned roles and responsibilities are not explicitly linked to the development, maintenance, and use of an ISE EA. Moreover, according to the Executive for Programs and Technology, his roles and responsibilities are currently under review and are subject to change. (2) The Program Manager previously served as the federal government's Chief Architect and as the Department of Justice (DOJ) Chief Architect. As such, the Program Manager possesses background and qualifications that span both the business and technology sides of the organization. (3) The Program Manager acts as the corporate spokesperson for the development and implementation of the ISE. For example, the current Program Manager has spoken in various public forums about the ISE since his appointment.

Appendix IV: ISE's Satisfaction of Selected EA Institutional Leadership and Management Controls

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>EA purpose is clearly stated. The purpose of the organization's EA drives virtually all aspects of how the EA program will be planned and executed, including the EA framework, methodology, plans, products, and tools. The purpose of an EA can range from consolidating the organization's IT infrastructure, to normalizing and integrating its data and promoting information sharing, to reengineering core business/mission functions and processes, to modernizing applications and sharing services, to modernizing the entire IT environment, and to transforming how the organization operates. Regardless of the purpose, which will in turn drive the expected value to be realized from the EA's implementation (e.g., reduced operating costs, enhanced ability to quickly and less expensively change to meet shifting external environment and new business demands/opportunities, improved alignment between operations and strategic goals and operations, etc.), it needs to be</p> <ul style="list-style-type: none"> (1) clearly defined by the executive committee; (2) communicated to and understood by all stakeholders and corporate and subordinate architecture staff; and (3) aligned with and supportive of the organization's overall strategic plan's goals, objectives, and outcomes. 	<p>Partially satisfied.</p> <p>The Office of the Program Manager has generally defined the purpose of the EAF, which is to guide the implementation of ISE capability. However, the Office of the Program Manager's Executive for Programs and Technology stated that the office does not plan to develop an ISE EA, and thus has not defined an ISE EA purpose.</p>
<p>EA framework(s) is adopted. To effectively and efficiently develop an EA, an organization should use an architecture framework, which can be viewed as an EA content taxonomy, to define the specification of the suite of EA products and artifacts to be developed, used, and maintained, and the relationships among them.</p>	<p>Partially satisfied.</p> <p>The ISE EAF describes and outlines the various levels of architecture that constitute the ISE architectural basis. In addition, it also outlines four key architecture views that the ISE is to address: business, data, applications and services, and technical. According to the ISE EAF, these views are to describe key attributes of the ISE to ensure that ISE strategic goals and objectives, business processes, investment, data, systems, services, and technologies are integrated and compatible with those across the federal government. However, the EAF does not provide the suite of specific architecture products and artifacts to be developed, used, and maintained, and the relationships among them.</p>

Appendix IV: ISE's Satisfaction of Selected EA Institutional Leadership and Management Controls

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>EA performance and accountability framework is established. Successfully managing any program, including an EA program, depends in part on establishing clear commitments and putting in place the means by which to determine progress against these commitments and hold responsible parties accountable for the results. Because the EA is a corporate asset, and its development and use are corporate endeavors involving a host of organizational players, a corporate approach for measuring EA progress, management capacity, quality, use, and results should be established that extends to all levels of the organization involved in the EA. In particular, it should</p> <p>(1) recognize the critical roles and responsibilities of key stakeholders, including the executive committee, the CIO, the chief architect, investment review board(s), and all subordinate committees and architects and</p> <p>(2) provide the metrics and means for ensuring that these roles and responsibilities are fulfilled and any deviations from expectations are documented and disclosed.</p>	<p>Partially satisfied.</p> <p>(1) The ISE EAF has defined the roles and responsibilities of ISE implementing agencies. For example, each ISE implementing agency must implement access authorization controls to protect shared data assets in accordance with the ISE's Identity and Access Management Framework. In addition, the Office of the Program Manager has established a performance framework that includes, among other things, objectives and activities associated with establishing aspects of the ISE architectural basis. For example, the performance framework states that ISE participants should fully integrate the ISE architecture program principles into their capital planning and investment control processes. In addition, the Program Manager's 2010 annual report describes, among other things, if ISE agencies are addressing these performance objectives and activities. However, the Office of the Program Manager has not developed an ISE EA and did not demonstrate that a corporate approach for ISE EA performance and accountability has been established. For example, the performance framework does not fully address accountability and performance monitoring based on dividing the planning, management, and implementation of an ISE EA among the Office of the Program Manager; each federal ISE member; state, local, and tribal entities; the private sector; and international partners.</p> <p>(2) The Office of the Program Manager's performance framework provides metrics for ensuring that certain roles and responsibilities of ISE implementing agencies and participating agencies are fulfilled. However, this performance framework is not associated with the development of an ISE EA.</p>
<p>EA program office(s) exists. EA development and maintenance should be managed as a formal program. Accordingly,</p> <p>(1) a corporate EA program management office should be chartered;</p> <p>(2) the program office should ensure EA program planning and performance monitoring;</p> <p>(3) the program office should ensure EA development and maintenance using supporting tools; and</p> <p>(4) the program office should ensure EA quality assurance, configuration management, and risk management.</p>	<p>Partially satisfied.</p> <p>(1) According to the Office of the Program Manager's Executive for Programs and Technology, a program office exists that includes both government and contractor staff who perform ISE architecture-related work. In addition, the Office of the Program Manager has issued the ISE EAF and other ISE architecture guidance. However, the office did not provide evidence to demonstrate that an EA program office responsible for developing and maintaining an ISE EA has been formally chartered.</p> <p>(2) The Office of the Program Manager did not provide evidence to demonstrate that an ISE EA program office is responsible for ISE EA program planning and performance monitoring.</p> <p>(3) The Office of the Program Manager did not provide evidence to demonstrate that an ISE EA program office is responsible for ISE EA development and maintenance using supporting tools.</p> <p>(4) The Office of the Program Manager did not provide evidence to demonstrate that an ISE EA program office is responsible for ISE EA quality assurance, configuration management, and risk management.</p>

**Appendix IV: ISE's Satisfaction of Selected EA
Institutional Leadership and Management
Controls**

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>EA development and maintenance methodology exists. An EA methodology defines the steps to be followed to generate and sustain the desired set of architecture artifacts, as identified in the EA framework(s). As such, the methodology or methodologies that corporate and subordinate program offices select and employ should</p> <p>(1) address how the architecture products provided for in the selected EA content framework will be developed and maintained to ensure that they are, among other things, consistent, complete, aligned, integrated, and usable;</p> <p>(2) be documented, understood, and consistently applied; and</p> <p>(3) provide the standards, tasks, tools, techniques, and measures to be followed in developing and maintaining the architecture products.</p>	<p>Partially satisfied.</p> <p>(1) The Office of the Program Manager has issued the EAF and the PAIS to guide, among other things, the development of agency-level ISSAs. For example, the PAIS provides high-level procedures for creating an ISE asset inventory. These documents provide guidance for developing elements of the agency-level ISSAs, but neither the ISE EAF nor the PAIS describes the sequence of ISE architecture products to be developed and how specific architecture products for the ISE EA (e.g., an ISE transition plan) will be developed and maintained to ensure that they are consistent, complete, aligned, integrated, and usable.</p> <p>(2) The EAF and PAIS have been documented. However, as described in this report, this guidance has not been consistently applied across the ISE implementing agencies.</p> <p>(3) Neither the EAF nor the PAIS provide the standards, tasks, tools, and techniques to be followed in developing and maintaining the ISE EA products.</p>
<p>Automated EA tools exist. Information about how the enterprise operates is captured and maintained in a variety of sources, such as the business vision statement, business strategy, performance and accountability plans and reports, policies, procedures, and guidance. Assimilating this information to support organizational transformation by creating a holistic view of the current and future state of the enterprise can be a challenging endeavor. Automated tools support this endeavor by assisting in the process of extracting, assimilating, relating, and presenting this organizational information. Automated EA tools can be used to</p> <p>(1) graphically and textually capture information described by the framework, such as information or activity models, and</p> <p>(2) assist in developing, communicating, storing, structuring, relating, accessing, and maintaining the architecture products described in the EA framework and methodology (e.g., business process models and data models).</p>	<p>Not satisfied.</p> <p>The Office of the Program Manager has not adopted automated EA tools to be used to develop an ISE EA.</p>

**Appendix IV: ISE's Satisfaction of Selected EA
Institutional Leadership and Management
Controls**

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>EA program management plan exists and reflects relationships with other management disciplines. An EA program management plan should describe the means by which the corporate EA program will be managed. As such, this plan should</p> <ul style="list-style-type: none"> (1) define the range of management structures, controls, disciplines, roles, and accountability mechanisms discussed throughout the EAMMF; (2) describe, at least notionally, the major EA releases or increments to be developed, and in doing so, should be aligned with the EA frameworks and methodologies to be employed; (3) be approved by the chief architect and the executive committee; (4) address how EA program management will be performed in concert with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control; and (5) be supported by subordinate plans that more specifically address key EA management areas, such as an organization communication plan, a human capital management plan, a configuration management plan, a risk management plan, and a quality assurance plan. 	<p>Not satisfied.</p> <p>The Office of the Program Manager has not established a program management plan to guide the development of an ISE EA. According to Office of the Program Manager officials, the office's approach to developing and defining the ISE architecture does not include developing such a plan because developing the ISE involves distributed activities across multiple agencies, and these activities are not owned by the office.</p>
<p>Work breakdown structure and schedule to develop EA exist. Each program management plan should</p> <ul style="list-style-type: none"> (1) be supplemented by a work breakdown structure that decomposes the specific tasks, activities, and events needed to execute the program and (2) provide a reliable schedule that defines the timing, sequencing, and duration of the tasks, activities, and events. The schedule not only provides a road map for the systematic execution of a program, but also provides the means by which to gauge progress, identify and address potential problems, and promote accountability. 	<p>Not satisfied.</p> <p>The Office of the Program Manager has not established a work breakdown structure to guide the development of an ISE EA. According to officials from the office, ISE schedules and milestones are under the purview of ISE mission partners and are described in internal agency-specific planning documents, which depend on resource allocation through the budget process.</p>

**Appendix IV: ISE's Satisfaction of Selected EA
Institutional Leadership and Management
Controls**

EAMMF element name and description	Analysis of ISE satisfaction of element
<p>EA segments, federation members, and/or extended members have been identified and prioritized. Organizations that adopt segmented or federated architecture approaches should identify and prioritize their subordinate or member architecture components.</p> <p>(1) The initial identification and prioritization of components should be performed by the corporate EA program office and approved by the executive committee.</p> <p>(2) Factors in identifying, prioritizing, and approving segments and federation members include</p> <ul style="list-style-type: none"> • strategic improvement opportunities; • needs and performance gaps; • organizational structures and boundaries, relevant legislation and executive orders; and • key component organizational and program dependencies. <p>(3) Organizations should ensure that these priorities are communicated throughout the enterprise.</p>	<p>Partially satisfied.</p> <p>(1) The Office of the Program Manager has identified five key priorities: building a national integrated network of fusion centers; continuing implementation of the Nationwide Suspicious Activity Reporting Initiative; establishing Sensitive but Unclassified/Controlled Unclassified Information network interoperability; improving governance of the classified National Security Information program; and advancing implementation of Controlled Unclassified Information policy. These priorities inform its crosscutting segment architecture priorities (e.g., SAR).</p> <p>(2) Office of the Program Manager's Executive for Programs and Technology stated that the office bases ISE priorities on gaps that are not already being addressed by other agencies activities. However, the office has not identified other segments (e.g., Cargo Screening), federation members' architectures (e.g., DOJ's EA), or extended members' architectures (e.g., international partners' EAs) that are to be developed as part of the ISE EA.</p> <p>(3) The Office of the Program Manager has communicated its priorities to agencies by describing them in its ISE 2010 annual report to Congress.</p>

Source: GAO analysis of ISE documents and interviews.

^aThis table refers to the ISE framework, which describes a discrete set of activities to be implemented under the ISE and includes a set of performance measures for these activities as well as a "maturity model" to gauge and track progress, as the ISE performance framework in order to distinguish it from the ISE EAF.

Appendix V: Analysis of Information Sharing Segment Architectures

Tables 3, 4, and 5 provide a summary of Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Justice (DOJ) efforts to address the key segment architecture development steps.

Table 3: DOD Satisfaction of Information Sharing Segment Architecture Development Steps

Step	Description	Satisfied?	Basis for determination
Launch project and determine participants	<p>(1) Launch information sharing segment architecture (ISSA) development project.</p> <p>(2) Identify relevant stakeholders.</p>	Yes	<p>(1) DOD demonstrated that it has launched its ISSA development effort. Specifically, it provided a November 2009 draft of its DOD Net-Centric ISSA.</p> <p>(2) DOD demonstrated that it has identified relevant stakeholders. Specifically, the draft ISSA includes the Office of Management and Budget, the General Services Administration, the Information Sharing Environment (ISE) Program Manager, and the Federal Bureau of Investigation as key stakeholders.</p>
Define the segment scope and strategic intent	<p>(1) Determine the scope to define information sharing segment boundaries.</p> <p>(2) Define the segment architecture's strategic intent.</p>	Yes	<p>(1) DOD demonstrated that it has defined the scope of its ISSA. Specifically, DOD's draft Net-Centric ISSA defines its information sharing scope as focusing on the DOD information enterprise architecture priorities related to (a) transforming DOD's approach from deployment of systems to the delivery of data and services and (b) securing data and services. The draft segment architecture also states that its scope will be limited to Suspicious Activity Reporting (SAR) information sharing for counterterrorism.</p> <p>(2) DOD demonstrated that it has defined the segment architecture's strategic intent. Specifically, the draft segment architecture provides DOD's target state vision and performance goals for information sharing. For example, DOD's vision describes a target state where transparent, open, agile, timely, relevant, and trusted information sharing occurs.</p>

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the business and information requirements	<p>(1) Describe the current environment that includes the current information flows and business and data architecture adjustments required to support sharing ISE mission-related information.</p> <p>(2) Document an asset inventory that identifies and categorizes assets (e.g., data assets, application and service assets) for sharing; identifies information exchanges for each SAR data asset to be shared; and identifies the risks associated with statutory or regulatory limitations or owners reluctance to share data assets.</p> <p>(3) Identify gaps within the data, application, and service layers of the segment architecture.</p>	Partial	<p>(1) DOD’s draft Net-Centric ISSA depicts a high-level “current” logical information flow for SAR-related activities (e.g., observation). However, it does not describe business and data architecture adjustments (e.g., mission business process reengineering) required to support sharing ISE mission-related information.</p> <p>(2) While the ISSA identifies assets that can support ISE implementation (e.g., NIPRNet and SIPRNet)^a and identifies the Federal Bureau of Investigation environment as DOD’s virtual shared space containing sharable SAR data, it does not include a complete data asset inventory or identify information sharing risks associated with statutory limitations. A senior DOD architecture official agreed with this assessment and stated that DOD’s Information Enterprise Architecture calls for establishing a data asset inventory. This official also stated that the risks associated with each asset are described in these assets’ supporting documentation.</p> <p>(3) The ISSA identifies data architecture gaps such as the need to establish a process for validating and verifying data schemas to eliminate data redundancies and ensure compliance, completeness, and accuracy.</p>
Define the conceptual solution architecture	<p>Define the conceptual solution architecture that</p> <p>(1) provides an integrated view of proposed systems and services, including the ISE core services and ISE members’ assets to be leveraged, and the connectivity between them;</p> <p>(2) takes into account gap analysis to determine if current systems and technologies satisfy target requirements; and</p> <p>(3) takes into account opportunities to reuse existing services and solutions.</p>	Partial	<p>(1) While the DOD Net-Centric ISSA identifies service-oriented architecture as an approach for defining a conceptual solution architecture, it does not provide an integrated view of proposed systems and services, including the ISE core services and ISE member assets to be leveraged, and the connectivity between them.</p> <p>(2) DOD did not provide evidence to demonstrate that its conceptual solution architecture takes into account a gap analysis of systems and technologies. According to a senior DOD architecture official, DOD has established a basis (e.g., the DOD information enterprise architecture, the Defense Architecture Registry System, and the DOD architecture framework) for identifying current systems and technologies that can satisfy target requirements.</p> <p>(3) DOD’s draft ISSA states that the DOD SAR information sharing initiative seeks to leverage the services and infrastructure of a third-party provider for establishing DOD’s virtual shared space.</p>

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the modernization blueprint	(1) Document implementation recommendations that are validated and approved by all stakeholders. (2) Include a transition plan that is focused on implementation of the information sharing recommendations.	Partial	(1) DOD's April 2009 Information Sharing Implementation Plan defines implementation recommendations, such as establishing an overarching governance structure for DOD enterprise information sharing and developing and improving data standards for exchanging basic information elements across the DOD enterprise. However, the draft did not include any evidence that the recommendations have been validated and approved by the key stakeholders. According to a senior DOD architecture official, the key stakeholders have opportunities to comment on DOD's implementation recommendations at monthly meetings, and none have disagreed with DOD's recommendations. (2) DOD did not provide evidence to demonstrate that it has developed a transition plan for its information sharing segment. While the implementation plan identifies specific actions to be taken (e.g., assess the operational effectiveness of information sharing activities) and goals to be achieved (e.g., ensure trust across organizations), it does not include a segment transition plan that provides timeframes for taking such actions.

Source: GAO analysis of DOD documents and interviews.

^aUnclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet).

Table 4: DHS Satisfaction of Information Sharing Segment Architecture Development Steps

Step	Description	Satisfied?	Basis for determination
Launch project and determine participants	(1) Launch information sharing segment architecture (ISSA) development project. (2) Identify relevant stakeholders.	Yes	(1) DHS demonstrated that it has launched its ISSA development effort. Specifically, the DHS ISSA dated May 2009 includes architecture artifacts such as an executive view, an architect view, and a program view. (2) DHS demonstrated that it has identified relevant stakeholders. Specifically, the ISSA identifies key stakeholders such as DHS; other federal agencies; state, local, tribal, territorial, and foreign governments; the intelligence community; and private and nongovernmental enterprises.

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the segment scope and strategic intent	<p>(1) Determine the scope to define information sharing segment boundaries.</p> <p>(2) Define the segment architecture's strategic intent.</p>	Yes	<p>(1) DHS demonstrated that it has defined the scope of its ISSA. Specifically, the ISSA defines its scope as the sharing of information within DHS and with its partners across the entire homeland security community, including other federal agencies; state, local, tribal, territorial, and foreign governments; and private and nongovernmental enterprises.</p> <p>(2) DHS demonstrated that it has defined the segment architecture's strategic intent. Specifically, the DHS ISSA indicates that the department's information sharing strategic intent is to effectively fight terrorism and respond to natural and man-made disasters.</p>
Define the business and information requirements	<p>(1) Describe the current environment that includes the current information flows and business and data architecture adjustments required to support sharing Information Sharing Environment (ISE) mission-related information.</p> <p>(2) Document an asset inventory that identifies and categorizes assets (e.g., data assets and application and service assets) for sharing; identifies information exchanges for each Suspicious Activity Reporting (SAR) data asset to be shared; and identifies the risks associated with statutory or regulatory limitations or owners reluctance to share data assets.</p> <p>(3) Identify gaps within the data, application, and service layers of the segment architecture.</p>	Partial	<p>(1) The DHS ISSA describes the current information flows for SAR and Alerts, Warnings, and Notifications (AWN) processes. However, it has yet to fully describe business and data architecture adjustments required to support the ISE. For example, while the ISSA states that DHS plans to streamline internal SAR processes to support the ISE, it has not made architecture adjustments to its business functions and policies to support the ISE and it does not plan to do so until ISE implementation guidance (e.g., for information discovery) is provided.</p> <p>(2) While the DHS ISSA provides a list of SAR data assets (e.g., Suspicious Incident Report Database), it does not include a list of AWN data assets. According to a DHS official, a list of AWN data assets has not been included in the ISSA because of a lack of definition of these terms by the Office of the Program Manager. Also, while the ISSA provides a list of SAR data assets, it does not identify risks described in existing information sharing agreements for these SAR assets. Further, the ISSA does not identify information exchanges for each SAR data asset to be shared. For example, it does not identify Information Exchange Packet Documentation for the Suspicious Incident Report Database.</p> <p>(3) DHS demonstrated that it has identified gaps. For example, the ISSA indicates a lack of ISE implementation guidance and milestones within the application and service layer of the ISSA.</p>

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the conceptual solution architecture	<p>Define the conceptual solution architecture that</p> <p>(1) provides an integrated view of proposed systems and services, including the ISE core services and ISE members' assets to be leveraged, and the connectivity between them;</p> <p>(2) takes into account gap analysis to determine if current systems and technologies satisfy target requirements; and</p> <p>(3) takes into account opportunities to reuse existing services and solutions.</p>	Partial	<p>(1) DHS did not provide evidence to demonstrate that it has defined a conceptual solution architecture that provides an integrated view of proposed systems and services, including the ISE core services and ISE members' assets to be leveraged, and the connectivity between them. According to DHS officials, efforts are under way to fully address this step.</p> <p>(2) DHS did not provide evidence to demonstrate that it has determined whether the current systems and technologies could satisfy target requirements.</p> <p>(3) DHS demonstrated that it plans to reuse existing services and solutions. For example, DHS plans to reuse the ISE core transport service, Identity and Access Management services, and standard exchange formats to access other federal, state, local, tribal, territorial, private and foreign information.</p>
Define the modernization blueprint	<p>(1) Document implementation recommendations that are validated and approved by all stakeholders.</p> <p>(2) Include a transition plan that is focused on implementation of the information sharing recommendations.</p>	Partial	<p>(1) According to DHS, ISSA recommendations have been validated and approved by all stakeholders. For example, DHS stated that its Information Sharing Governance Board has validated and approved the recommendation "Manage the implementation of DHS's information sharing architecture to guide development of a mature DHS Information sharing environment" as a key mission outcome to prevent terrorism and enhance security. In addition, the DHS ISSA has identified tasks (e.g., complete information requirements, business processes, and information flows for the law enforcement sharing segment) for achieving the target ISSA. However, DHS did not provide evidence to support that all recommendations have been validated by other relevant stakeholders, such as other federal agencies; state, local, and tribal governments; and private and nongovernmental enterprises.</p> <p>(2) DHS's ISSA included elements of a transition plan. For example, tasks related to information sharing are identified; however, the ISSA did not provide timelines for each task. According to DHS officials, efforts are under way to fully address this step.</p>

Source: GAO analysis of DHS documents and interviews.

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Table 5: DOJ Satisfaction of Information Sharing Segment Architecture Development Steps

Step	Description	Satisfied?	Basis for determination
Launch project and determine participants	(1) Launch information sharing segment architecture (ISSA) development project. (2) Identify relevant stakeholders.	Yes	(1) DOJ demonstrated that it has launched its ISSA development effort. Specifically, it provided ISSA documents dated May 2009. (2) DOJ demonstrated that it has identified key stakeholders, such as DOJ components; Information Sharing Environment (ISE) participants; and state, local, and tribal law enforcement agencies.
Define the segment scope and strategic intent	(1) Determine the scope to define information sharing segment boundaries. (2) Define the segment architecture's strategic intent.	Yes	(1) DOJ demonstrated that it has defined the scope of its ISSA. Specifically, DOJ's ISSA states that its information sharing scope encompasses DOJ mission operations and the department's relationships with external law enforcement organizations. (2) DOJ demonstrated that it has defined the segment architecture's strategic intent. Specifically, the ISSA states that the architecture's strategic intent is to transform the way DOJ shares law enforcement information with its federal and state, local, and tribal partners and create relationships and methods that allow information to be shared routinely across jurisdictional boundaries to prevent terrorism and systematically improve the investigation and prosecution of criminal activity.

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the business and information requirements	<p>(1) Describe the current environment that includes the current information flows and business and data architecture adjustments required to support sharing ISE mission-related information.</p> <p>(2) Document an asset inventory that identifies and categorizes assets (e.g., data assets and application and service assets) for sharing; identifies information exchanges for each Suspicious Activity Reporting (SAR) data asset to be shared; and identifies the risks associated with statutory or regulatory limitations or owners reluctance to share data assets.</p> <p>(3) Identify gaps within the data, application, and service layers of the segment architecture.</p>	Partial	<p>(1) DOJ demonstrated that it has described the current environment. Specifically, the ISSA describes business processes and information flows for end-to-end scenarios such as justice outreach, investigations and litigation, sentencing and corrections, and justice information services. In addition, it has identified the business and data architecture adjustments required to support sharing ISE-related information. For example, DOJ's SAR information flow diagram was modified to add activities such as posting SAR information to an ISE shared space.</p> <p>(2) While the ISSA identifies data assets related to specific DOJ business segments (e.g., the Drug Enforcement Administration's National Narcotics Intelligence System) and DOJ programs (e.g., criminal and noncriminal), DOJ did not provide a complete data asset inventory. For example, the DOJ ISSA does not identify the databases containing gun denial data. In addition, the ISSA identifies information exchanges (e.g., between the Justice Management Division's Joint Automated Booking System and the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System). Further, DOJ provided evidence that it has identified limitations associated with sharing data assets. For example, DOJ described limitations associated with assets for data publication and application access.</p> <p>(3) According to DOJ officials, the gaps are documented in the Justice Information Services Segment Architecture (JISSA). Although the JISSA was completed and provided to GAO, it was not completed and provided in time for consideration in this report.</p>

**Appendix V: Analysis of Information Sharing
Segment Architectures**

Step	Description	Satisfied?	Basis for determination
Define the conceptual solution architecture	<p>Define the conceptual solution architecture that</p> <p>(1) provides an integrated view of proposed systems and services, including the ISE core services and ISE members' assets to be leveraged, and the connectivity between them;</p> <p>(2) takes into account gap analysis to determine if current systems and technologies satisfy target requirements; and</p> <p>(3) takes into account opportunities to reuse existing services and solutions.</p>	Partial	<p>(1) DOJ demonstrated that it has defined a conceptual solution architecture that provides an integrated view of systems (e.g., OneDOJ) and the interfaces (e.g., Logical Entity Exchange Specification Publication and Discovery) between the systems. However, the integrated view does not specify ISE member-provided services and assets to be leveraged. According to DOJ officials, the JISSA includes information on services and assets used by DOJ and the broader justice community. However, DOJ did not provide the JISSA to us in time for consideration in this report.</p> <p>(2) DOJ did not provide evidence to demonstrate that it has determined if current systems, services, and technologies could satisfy the target business and information requirements. According to DOJ officials, the JISSA identifies opportunities to improve DOJ systems, services, and technologies to satisfy the business and information requirements. However, DOJ did not complete and provide the JISSA to us in time for consideration in this report.</p> <p>(3) DOJ demonstrated that it plans to reuse its existing services and solutions, such as the Logical Entity Exchange Specification.</p>
Define the modernization blueprint	<p>(1) Document implementation recommendations that are validated and approved by all stakeholders.</p> <p>(2) Include a transition plan that is focused on implementation of the information sharing recommendations.</p>	Partial	<p>(1) While the DOJ enterprise architecture (EA) transition strategy describes, among other things, a set of recommendations focused on information sharing (e.g., streamline information flows from external partners), it did not include evidence to demonstrate that all key stakeholders have approved and validated these recommendations.</p> <p>(2) DOJ does not have a transition plan for its information sharing segment, but it has an overall EA transition strategy that identifies planned investments and activities focused on implementation of the information sharing recommendations. For example, the EA transition strategy includes an activity to enhance existing DOJ proxy service capabilities to provide access to legacy systems, such as Interpol. It also provides descriptions of milestones for information sharing investments.</p>

Source: GAO analysis of DOJ documents and interviews.

Appendix VI: Comments from the Program Manager for the Information Sharing Environment

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

June 30, 2011

MEMORANDUM FOR: Eileen Larence
Director Homeland Security and Justice Issues
Government Accountability Office

SUBJECT: Draft GAO Report on the Information Sharing Environment (GAO-11-455)

Thank you for the opportunity to review the Draft Report on *the Information Sharing Environment*, GAO Report GAO-11-455. We value the engagement and interaction with respect to the Information Sharing Environment (ISE). While much has been accomplished, we agree with the GAO that there is still much to be done.

We generally agree with GAO's perspective on improving the Information Sharing Environment, as elaborated below. While the PM-ISE is given responsibilities to plan for, manage and oversee the approach to information sharing, it is OMB who provides both budgetary and architecture policy guidance to departments and agencies. Ultimately, it is the departments and agencies that manage the people, requirements, and systems and execute programs.

Recommendation 1: Leveraging the Community

With respect to leveraging agency initiatives, the Program Manager, Information Sharing Environment (PM-ISE) and the Information Sharing and Access Interagency Policy Committee (ISA IPC) have already leveraged a great number of initiatives that support the realization of the ISE. We will continue to identify and leverage agency initiatives to improve information sharing.

Examples of these initiatives include the following:

- Bureau of Justice Assistance (BJA) Global Justice Initiative – provides assistance to State and Local Law Enforcement in understanding and implementing the ISE;
- DOJ/FBI – Joint Terrorism Task Force (JTTF) – provides an FBI-sponsored multi-agency task force focused on the terrorism mission.
- BJA's State and Local Anti-Terrorism Training (SLATT) Program – delivers specialized terrorism / extremism orientation, interdiction, investigation, and prevention training to law enforcement agencies;
- FBI's eGuardian – a key federal component of the Nationwide Suspicious Activity Reporting Initiative;

Appendix VI: Comments from the Program Manager for the Information Sharing Environment

- BJA's Communities Against Terrorism Program – created to assist law enforcement in the development of partnerships with community members;
- Customs and Border Patrol's (CBP) Operational Integration Center near Detroit, Michigan, which supports and improves information sharing, threat assessment and joint response tactics between border security stakeholders in the Great Lakes region – provides partners with an overall view of Northern Border security status;
- BJA's Building Communities of Trust (BCOT) initiative – focuses on developing relationships of trust between police departments, fusion centers, and the communities they serve—particularly immigrant and minority communities—to prevent terrorist-related crime and to help keep communities safe;
- Domestic Nuclear Detection Office (DNDO) Securing the Cities (STC) – designs and implements a layered architecture for coordinated and integrated detection and interdiction of radiological materials that are out of regulatory control and may be used as a weapon within a metropolitan area;
- CBP's Port Radiation Inspection, Detection & Evaluation (PRIDE) Integration Program - connects Radiation Portal Monitors, Radioisotope Identification Devices data, and event metadata in an ever increasing number of CBP ports to a national database for analysis and central alert notification;
- DNDO West Coast Maritime Pilot (WCMP) – assesses capabilities that reduce vulnerabilities from nuclear and radiological weapons and materials delivered via small vessels across maritime borders;
- State Department - Russian Global Initiative to Combat Nuclear Terrorism (GICNT) – aims at strengthening international cooperation and collaboration in combating nuclear terrorism;
- DNDO Passenger/Bag Aviation Pilot – works with CBP to detect and interdict illicit nuclear and radiological weapons or materials entering the United States via the commercial aviation pathway; and
- Department of Commerce National Institute of Standards and Technology (NIST) establishing a program office for the National Strategy for Trusted Identities in Cyberspace – a critical element of managing the access to information.

For additional examples, please see the attached listing of ISE-leveraged activities (Attachment 1). For more examples, see the 2007 – 2010 annual reports available at www.ise.gov.

Recommendation 2: Defining Incremental Cost

With respect to defining incremental cost, we reinforce the point that the Office of Management and Budget (OMB) has the role of providing programmatic guidance and collecting budgetary requirements and ensuring they are integrated into the budget for each federal department and agency. It is also critical to note that the federal departments and agencies own, plan for, and manage their programs, systems and architectures, while PM-ISE provides the integrating guidance through the ISA IPC. Our ISE partners, the individual departments and agencies, have the responsibility to identify costs over and above their program baselines to extend the benefits of information sharing throughout the ISE.

Appendix VI: Comments from the Program Manager for the Information Sharing Environment

Recommendation 3: An Integrated Management Plan

We agree that the ISE needs an integrated plan with an established vision, goals, policy framework, performance management framework, and guidelines. In recent months, PM-ISE has worked with our mission partners to strengthen governance, engagement and alignment across ISE stakeholders. We are building capacity through increased emphasis on agency-based centers of excellence and are promoting a culture of continuous improvement and innovation. From a planning perspective, we begin with the 16 December 2005 Presidential memorandum. To this we add the current National Strategy on Information Sharing (NSIS), to be updated in the near future. The national strategy is followed by an integrated suite of implementation guidance and practices. Programmatic guidance, the policy framework, the budget and performance framework, the ISE Enterprise Architecture Framework, the Profile and Architecture Implementation Strategy (PAIS), and associated standards and guidelines provide the tools to effectively manage the ISE. We believe that through these documents, PM-ISE will establish the vision, a program management plan, and an executable roadmap for the ISE.

Much of the report treats the ISE as a centrally-designed and defined Information System Enterprise. The analysis looks for the tools and processes applicable to the procurement of such an enterprise. It is important to recognize that fundamentally, the ISE is not a single enterprise, but an approach to improving information sharing across multiple existing enterprises. As such, PM-ISE will work with the departments and agencies to identify and prioritize their projects in support of the Information Sharing Environment.

Other Observations and Comments:

Specific System Architecture Guidance

IRTPA states that the Information Sharing Environment is not a system or new set of systems; but is, instead, a "*decentralized, distributed*" approach to information sharing that utilizes, to the extent possible, the existing information system investments of the agencies. The ISE is intended to use common standards, processes and policies, but is not intended to create a single ISE system. By direction of law, the ISE "*builds upon existing systems capabilities currently in use across the Government,*" and leverages the existing infrastructures and information systems that support more than just the Counter-Terrorism mission. These department or agency information system investments are already controlled and directed by their own, broader Enterprise Architectures to meet their mission requirements.

The Program Manager for the Information Sharing Environment consulted with the main ISE agencies and they unanimously agreed that they do not need additional enterprise architecture guidance from the PM-ISE nor do they want or need the PM-ISE to develop an ISE Enterprise Architecture for them. It is appropriate for the PM-ISE to lead the update of the national strategy and associated implementation tools like the enterprise architecture framework, a policy framework, and a performance management framework; but, it is incumbent on agencies to develop their own enterprise architectures, budgets, investment plans, program management plans, and performance plans, in accordance with PM-ISE guidance. Agencies manage the programs that constitute the ISE; the PM-ISE does not. However, PM-ISE does work through

Appendix VI: Comments from the Program Manager for the Information Sharing Environment

the ISA IPC with departments and agencies to establish cross-cutting standards, segment architectures and functional standards in such areas as Suspicious Activity Reporting (SAR), which has been published; and Assured Sensitive But Unclassified (SBU) Interoperability, in work. We also support and leverage other cross-agency initiatives such as the National Information Exchange Model (NIEM), and Federal Identity, Credential, and Access Management (FICAM) activities.

The Roles and Responsibilities of OMB and the Federal Departments and Agencies

We are concerned that the draft report does not fully address the key roles played by OMB and each department and agency participating in the Information Sharing Environment. Given the questions contained in the original GAO engagement letter, dated October 23, 2009, we expected greater emphasis in the report on the role and participation of these key federal entities in the implementation of the ISE. Instead of addressing the understanding of the roles and responsibilities of the key federal entities, their progress, and accountability; over 25% of the body of the draft report and four of the appendices focus on the GAO Enterprise Architecture Management Maturity Framework (EAMMF). Recognizing the role played by OMB and the federal departments and agencies is key to the assessing progress in the ISE.

OMB plays a pivotal role in the planning, budgeting, and oversight of the federal agencies and their contributions to the ISE. It is primarily through the OMB – PM-ISE partnership that program direction, funding, and performance measurement can be effectively achieved. Departments and agencies are responsible for developing, deploying, modifying and maintaining their respective information system investments and associated Enterprise Architectures. They play an active role in determining the policies, priorities, and direction of the ISE, originally through the Information Sharing Council (ISC), and are an integral part of the ISA IPC. In addition, the information they share and the tools used to share it are, by their nature, a part of the ISE, regardless of whether or not the process is identified by PM-ISE.

Strategy Timeline

Please note that on page 15, the draft report states that the updated strategy is expected to be finalized in late-summer 2011. While this date was a notional projection, it is no longer valid. Drafting is actively underway, and this office is committed to completing the strategy. The planned issuance will be delivered once it has completed the Executive Branch process. When it is issued, however, we expect the updated Strategy, complemented by follow-on implementation policy, programmatic and budgetary guidance, and performance metrics to address many of the recommendations cited in this draft report.

We believe that the ISE Enterprise Architecture Framework informs departments and agencies of their technical responsibilities within the ISE. PM-ISE works with OMB to provide integrated, whole-of-government guidance and to establish a framework for departments and agencies information system investments within the ISE. This is accomplished as the components of the ISE, including existing information systems and associated investments,

**Appendix VI: Comments from the Program
Manager for the Information Sharing
Environment**

remain under the ownership and management authority of the individual departments and agencies. Anchored on the current National Strategy on Information Sharing and augmented by the planned Strategy update, we will provide a vision for the ISE. Programmatic guidance, policy, performance, management frameworks, and ISE standards and guidelines will provide the tools needed to effectively manage performance throughout the ISE. These tools, together with ISA IPC governance, and the commitment of departments and agencies, will support achieving a more robust Information Sharing Environment.



Kshemendra N. Paul

Attachment:

1. Leveraging Agency Initiatives

Appendix VII: Comments from the Department of Homeland Security

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



**Homeland
Security**

May 25, 2011

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

Re: Draft Report GAO-11-455, "INFORMATION SHARING ENVIRONMENT: Better Road Map Needed to Guide Implementation and Investments"

Dear Ms. Larence:

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

The Department is pleased to note the report recognizes that the Program Manager for the Information Sharing Environment (ISE) and key agencies, including DHS, have taken actions to define and implement the ISE, such as developing a framework to advance an initial set of goals, activities, and actions.

Although the report does not contain recommendations specifically directed at DHS, the Department remains committed to continuing its work with the Program Manager and relevant stakeholders to further define and implement a fully functioning ISE. For example, the Department is actively engaged with the Program Manager on a number of key initiatives at the Information Sharing and Access Interagency Policy Committee to ensure the realization of information-sharing benefits government-wide. These include the work being undertaken by the Watchlisting and Screening, Fusion Center, Privacy and Civil Liberties, Suspicious Activity Reporting and Information Integration Subcommittees, and their associated working groups.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments on the draft report have been provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim H. Crumpacker".

Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

Appendix VIII: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Eric Erdman, Assistant Director; Anh Le, Assistant Director; David Alexander; Justin Booth; R.E. Canjar; Katherine Davis; R. Denton Herring; Michael Holland; Ashfaq Huda; Thomas Lombardi; Linda Miller; Victoria Miller; Krzysztof Pasternak; Karl Seifert; Adam Vodraska; and Michelle Woods 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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

