United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2007

INFORMATION TECHNOLOGY

DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments

GAO-07-424

April 2007

INFORMATION TECHNOLOGY

DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-424, a report to congressional requesters

Why GAO Did This Study

The Department of Homeland Security (DHS) relies extensively on information technology (IT) to carry out its mission. For fiscal year 2008, DHS requested about $4 billion—the third largest planned IT expenditure among federal departments. Given the size and significance of DHS's IT investments, GAO's objectives were to determine whether DHS (1) has established the management structure and associated policies and procedures needed to effectively manage these investments and (2) is implementing key practices needed to effectively control them. GAO used its IT Investment Management (ITIM) framework and associated methodology to address these objectives, focusing on the framework's stages related to the investment management provisions of the Clinger-Cohen Act.

What GAO Recommends

GAO recommends that DHS fully define the project-level and portfolio-level policies and procedures defined in GAO's ITIM framework and implement the practices needed to effectively control investments. In written comments on this report, DHS agreed with GAO's findings and recommendations and stated it will use the report to improve its investment management process.

www.gao.gov/cgi-bin/getrpt?GAO-07-424.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

DHS has established the management structure to effectively manage its investments. However, the department has yet to fully define 8 of the 11 related policies and procedures that GAO's ITIM framework defines (see the table below). Specifically, while DHS has documented the policies and related procedures for project-level management, some of these procedures do not include key elements. For example, procedures for selecting investments do not cite either the specific criteria or steps for prioritizing and selecting new IT proposals. In addition, the department has yet to define most of the policies associated with managing its IT projects as investment portfolios. Officials attributed the absence of policies and procedures at the portfolio level to other investment management priorities. Until DHS fully defines and documents policies and procedures for investment management, it risks selecting investments that will not meet mission needs in the most cost-effective manner.

DHS has also not fully implemented the key practices needed to actually control investments—either at the project level or at the portfolio level. For example, according to DHS officials and the department's control review schedule, DHS investment boards have not conducted regular investment reviews. Further, while GAO found that control activities are sometimes performed, they are not performed consistently across projects. In addition, because the policies and procedures for portfolio management have yet to be defined, control of the department's investment portfolios is ad hoc, according to DHS officials.

Officials told GAO that they have recently hired a portfolio manager and are recruiting another one to strengthen IT investment management. Until DHS fully implements processes to control its investments, both at the project and portfolio levels, it increases the risk of not meeting cost, schedule, benefit, and risk expectations.

Execution of Policy and Procedure-Related Key Practices in GAO's Framework

Stage 2: building the investment foundation	Key practices executed	Stage 3: developing a complete investment portfolio	Key practices executed
Instituting the investment board	1/1	Defining the portfolio criteria	0/1
Meeting business needs	1/1	Creating the portfolio	0/1
Selecting an investment	1/3	Evaluating the portfolio	0/1
Providing investment oversight	0/1	Conducting postimplementation reviews	0/1
Capturing investment information	0/1		
Overall	3/7		0/4

Source: GAO.

Contents

Figures

Abbreviations

APB	Acquisition Program Baseline
CFO	Chief Financial Officer
CIO	Chief Information Officer
eNEMIS	National Emergency Management Information System
DHS	Department of Homeland Security
EAB	Enterprise Architecture Board
IPRT	Integrated Project Review Team
IRB	Investment Review Board
IT	information technology
ITIM	IT Investment Management
IWN	Integrated Wireless Network
JRC	Joint Requirements Council
OA	operational analysis
PIR	postimplementation review
TWIC	Transportation Worker Identification Credentialing

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

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 27, 2007

The Honorable Robert C. Byrd
Chairman
The Honorable Thad Cochran
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable David E. Price
Chairman
The Honorable Harold Rogers
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The Department of Homeland Security (DHS) is one of the largest federal agencies in the government. With its workforce of over 200,000 employees and budget of $42.7 billion, it manages numerous information technology (IT) programs to carry out its mission of leading the unified national effort to secure America by preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the nation. Specifically, for fiscal year 2008, DHS requested about $4 billion for IT—the third largest planned IT expenditure among federal departments.[1]

This report is one of a series of products to respond to DHS's fiscal year 2006 appropriations act. The act directs the department's Chief Information Officer (CIO) to submit a report to congressional appropriations committees that includes, among other things, a description of the department's IT capital planning and investment control process. The act also directs us to review the report.[2] As agreed with your offices, our objectives were to determine whether DHS (1) has established

[1]Office of Management and Budget, *Fiscal Year 2008 Report on Information Technology Budgets* (Washington, D.C.: Feb. 6, 2007).

[2]As part of this mandate, we are also reviewing the department's enterprise architecture and IT human capital strategy.

the management structure and associated policies and procedures needed to effectively manage its IT investments and (2) is implementing key practices needed to effectively control them. To address our objectives, we evaluated DHS's documented policies and procedures for making IT investment management decisions and DHS's processes for controlling investments against the accepted practices presented in our IT Investment Management framework (ITIM). This framework provides a method for assessing how well an agency is managing its IT resources.[3] We focused on the project-level and portfolio-level key practices that assist organizations in establishing the selection, control, and evaluation processes required by the Clinger-Cohen Act of 1996.[4] Specifically, we addressed the 11 key practices that are policy and procedure-related. Of these 11 practices, 7 are project-level practices, and 4 are portfolio-level practices. We also addressed the key practices associated with controlling investments and portfolios.

We performed our work from February 2006 through March 2007 in accordance with generally accepted government auditing standards. Appendix I contains details about our objectives, scope, and methodology.

Results in Brief

DHS has established the management structure to effectively manage its investments. However, the department has yet to fully define 8 of the 11 related policies and procedures defined by our ITIM framework. Specifically, while DHS has documented the policies and the related procedures for project-level management, some of these procedures do not include key elements. For example, procedures for selecting investments do not cite either the specific criteria or steps for prioritizing and selecting new IT proposals, and procedures for management oversight of IT projects and systems do not specify the rules the investment boards are to follow in controlling investments. In addition, the department has yet to define most of the policies associated with managing its IT projects as investment portfolios. Officials attributed the absence of policies and procedures at the portfolio level to other investment management priorities. Until DHS fully defines and documents policies and procedures for investment management, it risks selecting investments that will not meet mission needs in the most cost-effective manner.

[3]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

[4]The Clinger-Cohen Act of 1996, 40 U.S.C. §§ 11311–11313.

DHS has also not fully implemented any of the key practices needed to actually control investments—either at the project level or at the portfolio level. For example, according to DHS officials and the department's control review schedule, the investment boards have not conducted regular reviews of investments. While control activities are sometimes performed, they are not performed consistently across all IT projects. In addition, because the policies and procedures for portfolio management have yet to be defined, control of the department's investment portfolios is ad hoc, according to DHS officials. To strengthen IT investment management, officials told us that they have recently hired a portfolio manager and are recruiting another one. Until DHS fully implements processes to control its investments, both at the project and portfolio levels, it increases the risk that its projects will not meet cost, schedule, benefit, and risk expectations.

To strengthen DHS's investment management capability, we are recommending that the department devote the appropriate degree of attention to fully defining the project-level and portfolio-level policies and procedures in our ITIM framework and implementing those framework practices needed to control investments at both the project level and the portfolio level. In commenting on a draft of this report, the department agreed with our findings and recommendations and stated it will use the report to improve its investment management and review processes.

Background

Since beginning operations in March 2003, DHS has assumed operational control of about 209,000 civilian and military positions from 22 agencies and offices specializing in one or more aspects of homeland security.[5] The intent behind DHS's merger and transformation was to, among other things, improve coordination, communication, and information sharing among the multiple federal agencies responsible for carrying out the mission of protecting the homeland.

Overview of DHS Organizational Structure

To accomplish its mission, the department is organized into various components, each of which is responsible for specific homeland security missions and for coordinating related efforts with its sibling components,

[5]Some of those specialties are intelligence analysis, law enforcement, border security, transportation security, biological research, critical infrastructure protection, and disaster recovery.

as well as external entities. Table 1 shows DHS's principal organizations and their missions. An organizational structure is shown in figure 1.

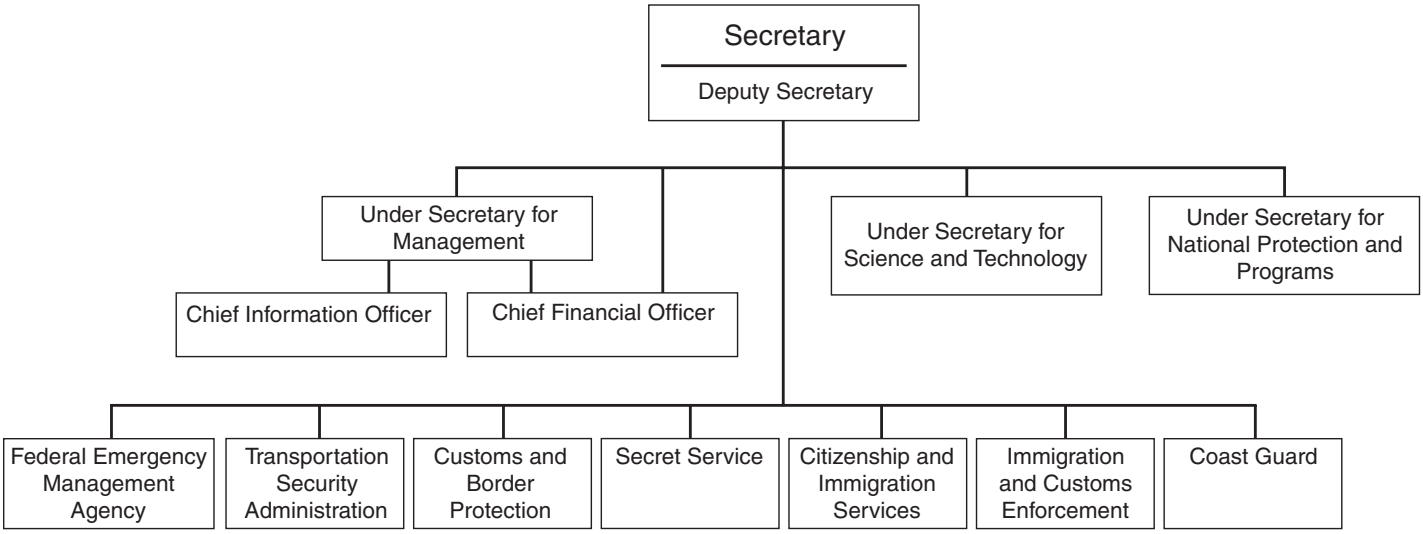
Table 1: DHS's Principal Organizations and Their Missions

Principal organizations[a]	Missions
Citizenship and Immigration Services	Administers immigration and naturalization adjudication functions and establishes immigration services policies and priorities.
Coast Guard	Protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, and in any maritime region as required to support national security.
Customs and Border Protection	Secures the nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Federal Emergency Management Agency	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
Immigration and Customs Enforcement	Investigates, identifies, and addresses vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Management Directorate	Is responsible for department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, IT systems, facilities and equipment, and the identification and tracking of performance measurements. This directorate includes the Offices of the Chief Financial Officer and the CIO.
National Protection and Programs Directorate	Supports the department's homeland security risk reduction mission through an integrated approach that encompasses both physical and virtual threats and their associated human elements. This directorate includes the Offices of Cyber Security and Communications and Infrastructure Protection.
Science and Technology Directorate	Serves as the primary research and development arm of the department, responsible for providing federal, state, and local officials with the technology and capabilities to protect the homeland.
Secret Service	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes (including financial institution fraud, identity theft, and computer fraud) and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.
Transportation Security Administration	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.

Sources: GAO analysis of DHS data.

[a]This table does not show the organizations that fall under each of the directorates. This table also does not show all organizations that report directly to the DHS Secretary and Deputy Secretary, such as Executive Secretary, Legislative and Intergovernmental Affairs, Public Affairs, Chief of Staff, Inspector General, and General Counsel.

Figure 1: DHS Organizational Structure (Simplified and Partial)



Source: GAO analysis of DHS data.

Within the Management Directorate is the Office of the CIO, which is expected to leverage best available technologies and IT management practices, provide shared services, coordinate acquisition strategies, maintain an enterprise architecture that is fully integrated with other management processes, and advocate and enable business transformation. Other DHS entities also are responsible or share responsibility for critical IT management activities. For example, DHS's major organizational components (e.g., directorates, offices, and agencies) have their own CIOs and IT organizations. Control over the department's IT funding is vested primarily with the components' CIOs, who are accountable to the heads of their respective components.[6] The Director of Program Analysis and Evaluation is the sponsor for the department's capital planning and investment control process and serves as the executive agent and coordinator for the process. This Director reports to the Chief Financial Officer (CFO).

[6]GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-715T (Washington, D.C.: May 8, 2003).

IT Is Critical to DHS's Mission Performance

To accomplish its mission, DHS relies extensively on IT. For example, for fiscal year 2007 DHS requested about $4.16 billion to support 278 major IT programs. Table 2 shows the fiscal year 2007 IT funding for key DHS components.

Table 2: IT Funding for Fiscal Year 2007

Dollars in millions	
DHS components and investments	**Funding**
Citizenship and Immigration Services	$570.3
Coast Guard	196.7
Customs and Border Protection	546.4
Federal Emergency Management Agency	77.1
Immigration and Customs Enforcement	134.0
Management Directorate	
Enterprise Application Delivery[a]	20.7
Enterprise Architecture and Investment Management Program[b]	35.6
Enterprise-Geospatial System[c]	12.8
Homeland Secure Data Network[d]	32.7
Human Resources IT[e]	19.1
Information Security Program[f]	57.8
Integrated Wireless Network[g]	361.3
Watch List and Technical Integration[h]	9.9
CIO Office salaries and expenses	16.5
Other IT infrastructure[i]	954.3
Other	55.3
Preparedness Directorate[j]	213.5
Science and Technology Directorate	34.1
Secret Service	3.8
Transportation Security Administration	356.4
US-VISIT[k]	407.4
Other DHS components	45.1
Total	**$4,160.8**

Source: GAO analysis of DHS data.

[a]Enterprise Application Delivery is to consolidate existing and planned Web pages and platforms of the DHS component organizations.

[b]The Enterprise Architecture and Investment Management Program is to develop the department's enterprise architecture and implement the transition strategy through the department's investment management process.

[c]The Enterprise-Geospatial System is to establish a framework, organizational structure, and requisite resources to enable departmentwide use of geographic information systems.

[d]The Homeland Secure Data Network is to merge disparate classified networks into a single, integrated network to enable, among other things, the secure sharing of intelligence and other information.

[e]Human Resources IT includes the set of DHS enterprisewide systems to support personnel regulations

[f]The Information Security Program is to establish information security policies and procedures throughout the department to protect the confidentiality, integrity, and availability of information.

[g]The Integrated Wireless Network is to deliver the wireless communications services required by agents and officers of DHS, the Department of Justice, and the Department of the Treasury.

[h]Watch List and Technical Integration is to increase effective information sharing by consolidating, re-using, and retiring applications that develop multiple terrorist watch lists being used by multiple operating entities within the government.

[i]Other infrastructure includes initiatives with the goal of creating a single, consolidated, and secure infrastructure to ensure connectivity among the department's 22 component organizations.

[j]On April 1, 2007, this Directorate was replaced by the National Protection and Programs Directorate.

[k]On April 1, 2007, US-VISIT became part of the National Protection and Programs Directorate.

As mentioned earlier, DHS requested about $4 billion for fiscal year 2008, which is the third largest planned IT expenditure among federal departments.

Prior GAO Reviews of DHS's IT Investment Management Efforts

During the last 3 years, we have reported on steps that DHS has taken to establish its IT investment management activities and the associated challenges it faced.

- In May 2004, we reported that DHS was in the midst of developing and implementing a strategic approach to IT management.[7] We also reported that DHS's interim efforts to manage IT investments did not provide assurance that those investments were strategically aligned. As a result, we concluded that DHS system investments were at risk of requiring rework in order to properly align with strategic mission goals and outcomes. Accordingly, we recommended that DHS limit its IT investments to those efforts that were deemed cost-effective via several criteria and considering any future system rework that would be needed to later align the system with the department's emerging systems integration strategy.

[7]GAO, *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems*, GAO-04-509 (Washington, D.C.: May 21, 2004).

- In August 2004, we reported that DHS had established several key foundational elements for investment management.[8] However, we also reported that DHS was not providing effective departmental oversight of IT investments, with many investments not receiving control reviews, due in large part to the lack of an organized process for conducting the reviews. Accordingly, we recommended that DHS establish milestones for the initiation and completion of major information and technology management activities, such as conducting these control reviews.

- In March 2006, we testified that DHS had worked to institutionalize IT management controls across the department but still faced challenges.[9] We identified actions that DHS reported it was taking, while noting, for example, that the department still needed to define explicit criteria for determining if investments aligned with the agency's modernization road map (enterprise architecture).

Overview of DHS's Approach to Investment Management

DHS's enterprisewide and component agency IT investments are categorized into one of four "levels" of investments that determine the extent and scope of the required project and program management, the level of reporting requirements, and the review and approval authority. An investment is assigned to a level based on its total acquisition costs and total life cycle costs.[10] Table 3 shows the dollar thresholds that DHS reports it uses in determining investment levels.

Table 3: Levels of Investments

Level	Acquisition costs	Life cycle costs
1	Greater than $100 million	Greater than $200 million
2	Between $50 and $100 million	Between $100 and $200 million
3	Between $20 and $50 million	Between $50 and $100 million
4	Less than $20 million	Less than $50 million

Source: DHS documents.

[8]GAO, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004).

[9]GAO, *Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology*, GAO-06-598T (Washington, D.C.: Mar. 29, 2006).

[10]Investments may be assigned to a higher level for certain reasons, including high development, operating, or maintenance costs or high executive visibility.

Several entities and individuals are involved in managing these investments. Table 4 lists the decision-making bodies and personnel involved in DHS's investment management process, and provides a description of their key responsibilities and membership.

Table 4: DHS Governance Entities and Responsibilities

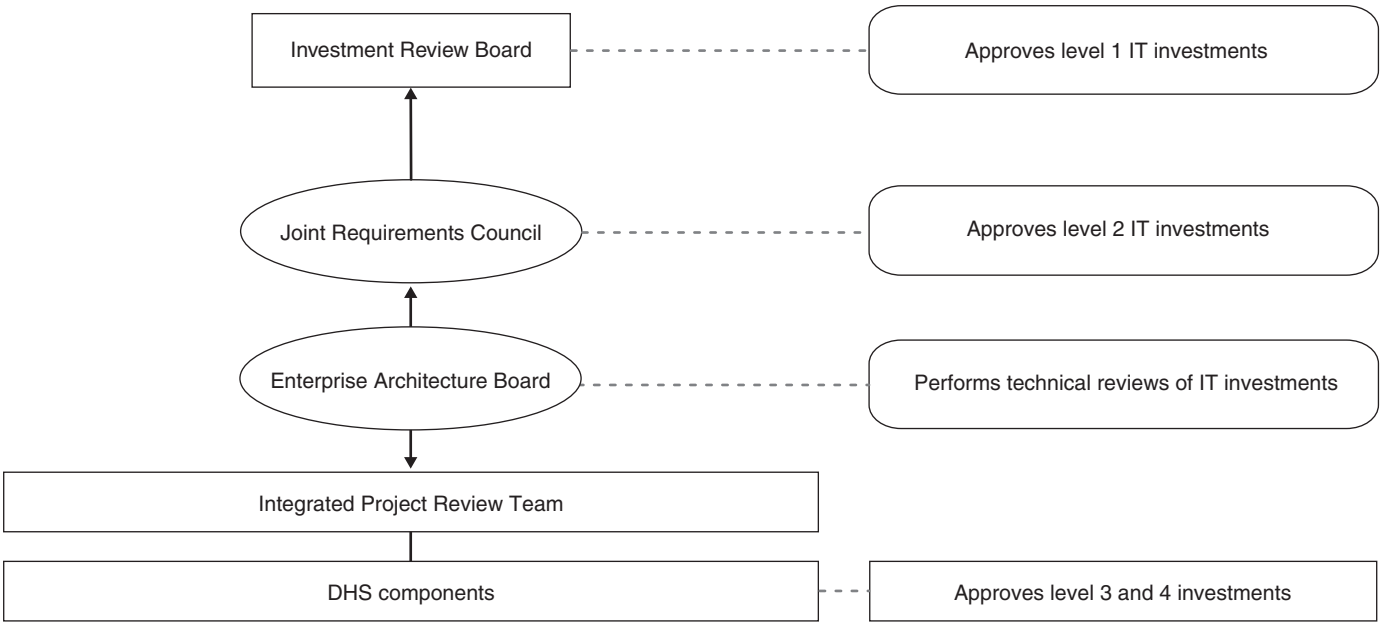
Governance entity	Membership/description	Example of responsibilities
Investment Review Board (IRB)	Chaired by the Deputy Secretary. Members are the Under Secretary for Management and other senior executives, including the CIO, CFO, Chief Procurement Officer, and the Director for Program Analysis and Evaluation. The chair of the Joint Requirements Council holds an adjunct member position.	• Approves level 1 investments. • Reviews and validates portfolio placement. • Provides strategic guidance for the Joint Requirements Council.
Joint Requirements Council (JRC)	Chair appointed by the Deputy Secretary from among the JRC members. Members include the Chief of Staff, DHS Management; Chief of Staff, Policy; the Chief Procurement Officer, Chief Information Officer, and senior managers from each business component.	• Approves level 2 investments. • Provides recommendations to the IRB for level 1 investments regarding requirements, risk, effect on the mission and other department programs, and ability to implement within the project spending plan. • Conducts portfolio reviews and determines the appropriate portfolio for investments. • Validates requirements.
Enterprise Architecture Board (EAB)	Chaired by CIO. Members are CIOs from component entities, business unit and program representatives, and CFO, Chief Procurement Officer, Chief Administrative Officer designees.	• Oversees the department's enterprise architecture. • Performs technical reviews of level 1 and level 2 IT investments. • Reviews level 3 and level 4 for IT elements at the inception of the investment and annually.
Heads of components	Chief Operating Officer or his/her designee.	• Approves all level 3 and 4 investments. • Conducts appropriate management and oversight of investments and establishes processes to manage approved investments at the component level.
Program Analysis and Evaluation Office (This office is part of the Office of the CFO.)	Director serves as the DHS's executive agent and coordinator for the investment review process.	• Reviews investments and prepares decision support information and analysis for the IRB and JRC. • Coordinates activities of the Integrated Project Review Team and adjudicates review issues.

Governance entity	Membership/description	Example of responsibilities
Integrated Project Review Team	Led by Program Analysis and Evaluation Office. Members include subject matter experts from appropriate functional disciplines and representatives from the following offices: CIO, CFO, Privacy, Policy, Security, Chief Procurement Officer, Chief Administrative Officer, General Counsel, and Science and Technology.	• Is the entry point for the investment management process. • Provides technical guidance on the process and the investments. • Conducts integrated investment reviews in support of the IRB, JRC, and EAB. • Performs comprehensive decision milestones and portfolio reviews for level 1 and 2 investments. • Guides components in a portfolio analysis of their investments.

Source: GAO analysis of DHS data.

Figure 2 shows the relationship among the key players in DHS's investment management process.

Figure 2: DHS Review and Approval Process



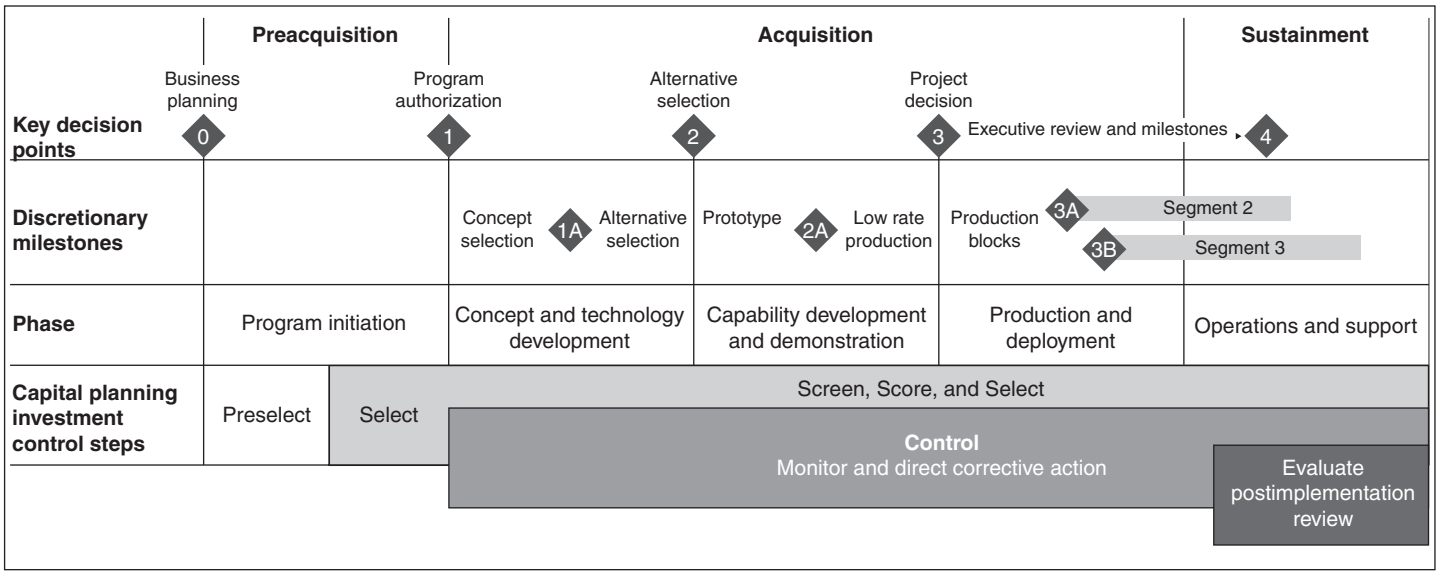
Source: DHS.

Investment Management Process

DHS's investment management process consists of four phases (which it refers to as Capital Planning Investment Control Steps): (1) the *preselect phase* supports the initial conception and development of the investment, (2) the *select phase* supports the selection of the investment from among competing investments, (3) the *control phase* supports the monitoring of

investments for acceptable performance, and (4) the *evaluate phase* supports the evaluation of investments for progress made against objectives. Each phase of the process is made up of multiple steps that set out requirements that need to be met in order for the boards to make decisions about the investments. The investment management phases are aligned with projects' life cycle phases, as illustrated in figure 3.[11] According to DHS policy, the boards are to review projects at key decision points or at least annually. Figure 3 shows where these key decision points (see shaded areas) are to occur in a project's life cycle and in the investment management process.

Figure 3: DHS Investment Review Process



Source: DHS.

Preselect

DHS's preselect phase is to identify the business needs and assess the preliminary costs and benefits needed for the development and support of an investment's initial concept. During this phase, the component agency is to assign a project manager to develop an investment review request—

[11]DHS's systems development life cycle has five stages: (1) Project Initiation, (2) Concept and Technology Development, (3) Capability Development and Demonstration, (4) Production and Deployment, and (5) Operations and Support.

essentially an investment proposal—and to scope the project. The document is to provide initial information, which is to be used to establish a schedule for the investment's key milestone reviews and be reviewed by the Integrated Project Review Team (IPRT). For major investments (level 1 and 2 investments), project managers are required to also assemble an interdisciplinary team to assist in the management of the investment. During this phase, the EAB assesses investments for alignment with the enterprise architecture and provides recommendations to the appropriate decision-making authorities (recommendations for level 1 investments are made to the IRB, those for level 2 investments are made to the JRC, and those for level 3 and 4 investments are made to the heads of the components). Project managers present investment proposals to their component-level investment review boards for approval.

Select

In the select phase, DHS is to assess investments against a uniform set of evaluation criteria and thresholds to ensure that the department selects the investments that best support its mission. All new and existing investments are to go through this phase in support of DHS's annual programming and budgeting process. Based on the assessments during the select phase, DHS is to prioritize investments and decide which investments to include in its portfolios. The select phase is also intended to help the department justify budget requests by demonstrating the resources required for individual investments. At the end of the selection process, the department is to produce a scored and ranked list of Exhibit 300s[12] for all major investments and an Exhibit 53[13] for all level 1 through level 4 IT investments for submission to the Office of Management and Budget.

Control

Once resources are expended to acquire planned capabilities, the investment is assumed to be in the control phase, and control related activities are to continue throughout the investment's life cycle. During this phase, project managers are responsible for preparing inputs for

[12]Exhibit 300 is a capital asset plan completed for major IT systems and IT budget initiatives.

[13]Exhibit 53 is the listing of all IT investment, providing budget estimates for overall IT investments and for major and significant IT systems.

periodic reporting in support of investment reviews. The purpose of the reviews is to ensure that investments are performing within acceptable cost, schedule, and performance parameters. The Acquisition Program Baseline is the main control instrument used through predeployment to baseline these parameters for investments. The IPRT reviews the Acquisition Program Baseline and other periodic reporting documents and provides recommendations to the project teams, if needed. Once the project teams have made the recommended changes, the IPRT provides a summary package to the component agency heads and DHS's review boards (IRB and JRC) to support key milestone decision reviews and other reviews established in the investment's investment review request during the preselect phase.

Evaluate

The evaluate phase begins when an investment is implemented or is deployed and operational. During this phase, project managers are responsible for conducting postimplementation reviews (PIR) to evaluate the impact of the investment on the department's mission and programs. The PIR focuses on three primary areas: impact to stakeholders and customers, ability to deliver results, and ability to meet baseline goals. Major investments that are in the operations and maintenance phases are required to perform an operational analysis to measure performance and cost against the investment's baseline. If the investment's performance is deficient, the program manager is required to introduce corrective actions. Any changes to the investment's original baseline need to be approved by the appropriate IRB. The lessons learned from conducting a PIR are to be reported to the IPRT for use throughout the department.

Overview of GAO's ITIM Maturity Framework

The ITIM framework consists of five progressive stages of maturity that an agency can achieve in its investment management capabilities.[14] It was developed on the basis of our research into the IT investment management practices of leading private- and public-sector organizations. The maturity stages are cumulative; that is, in order to attain a higher stage, an agency must institutionalize all of the critical processes at the lower stages, in addition to the higher stage critical processes.

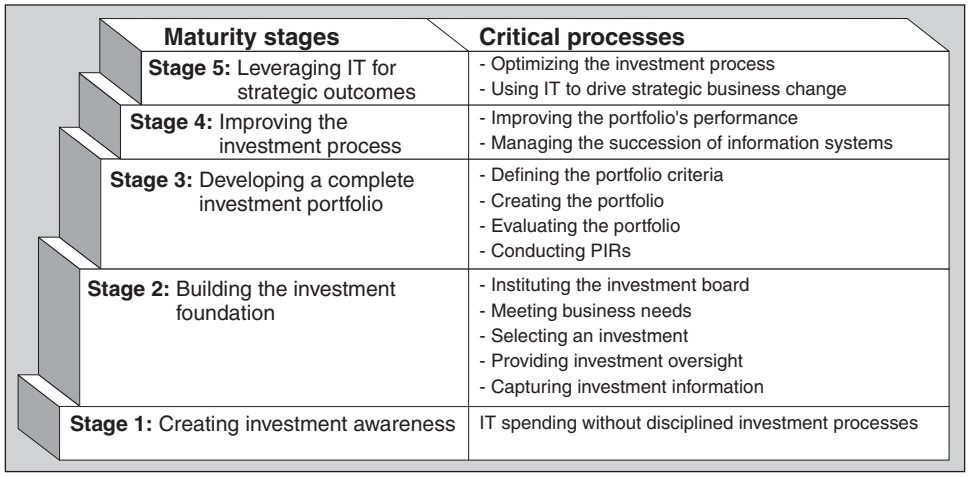
[14] GAO-04-394G.

The framework can be used to assess the maturity of an agency's investment management processes and as a tool for organizational improvement. The overriding purpose of the framework is to encourage investment processes that promote business value and mission performance, reduce risk, and increase accountability and transparency in the decision process. We have used the framework in several of our evaluations,[15] and a number of agencies have adopted it. These agencies have used ITIM for purposes ranging from self-assessment to redesign of their IT investment management processes.

ITIM's five maturity stages (see fig. 4) represent steps toward achieving stable and mature processes for managing IT investments. The successful attainment of each stage leads to improvement in the organization's ability to manage its investments. With the exception of the first stage, each maturity stage is composed of "critical processes" that must be implemented and institutionalized in order for the organization to achieve that stage. These critical processes are further broken down into key practices that describe the types of activities that an organization should be performing to successfully implement each critical process. It is not unusual for an organization to be performing key practices from more than one maturity stage at the same time. However, our research shows that agency efforts to improve investment management capabilities should focus on implementing all lower stage practices before addressing higher stage practices.

[15]GAO, *Information Technology: DLA Needs to Strengthen Its Investment Management Capability*, GAO-02-314 (Washington, D.C.: Mar. 15, 2002); *United States Postal Service: Opportunities to Strengthen IT Investment Management Capabilities*, GAO-03-3 (Washington, D.C.: Oct. 15, 2002); *Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior*, GAO-03-1028 (Washington, D.C.: Sept. 12, 2003); *Bureau of Land Management: Plan Needed to Sustain Progress in Establishing IT Investment Management Capabilities*, GAO-03-1025 (Washington, D.C.: Sept. 12, 2003); and *Information Technology: FAA Has Many Investment Management Capabilities in Place, but More Oversight of Operational Systems Is Needed*, GAO-04-822 (Washington, D.C.: Aug. 20, 2004); *Information Technology: HHS Has Several Investment Management Capabilities in Place, but Needs to Address Key Weaknesses*, GAO-06-11 (Washington, D.C.: Oct. 28, 2005); *Information Technology: Centers for Medicare & Medicaid Services Needs to Establish Critical Investment Management Capabilities*, GAO-06-12 (Washington, D.C.: Oct. 28, 2005).

Figure 4: The Five ITIM Stages of Maturity with Critical Processes



Source: GAO.

In the ITIM framework, Stage 2 critical processes lay the foundation for sound IT investment processes by helping the agency to attain successful, predictable, and repeatable investment control processes at the project level. At Stage 2, the emphasis is on establishing basic capabilities for selecting new IT projects, and on developing the capability to (1) control projects so that they finish predictably within established cost, schedule, and performance expectations and (2) identify and mitigate potential exposures to risk.

Stage 3 is where the agency moves from project-centric processes to portfolio-based processes and evaluates potential investments by how well they support the agency's missions, strategies, and goals. This stage requires that an organization continually assess both proposed and ongoing projects as parts of complete investment portfolios—integrated and competing sets of investment options. It focuses on establishing a consistent, well-defined perspective on IT investment portfolios and maintaining mature, integrated selection (and reselection), control, and evaluation processes, which are to be evaluated during PIRs. This portfolio perspective allows decision makers to consider the interaction among investments and the contributions to organizational mission goals and strategies that could be made by alternative portfolio selections, rather than to focus exclusively on the balance between the costs and benefits of individual investments. Organizations implementing Stage 2 and 3 key practices have in place capabilities that assist in establishing the

selection, control, and evaluation processes required by the Clinger-Cohen Act of 1996.[16]

Stages 4 and 5 require the use of evaluation techniques to continuously improve both investment processes and portfolios in order to better achieve strategic outcomes. At Stage 4 maturity, an organization has the capacity to conduct IT succession activities and, therefore, can plan and implement the deselection of obsolete, high-risk, or low-value IT investments. An organization with Stage 5 maturity conducts proactive monitoring for breakthrough technologies that will enable it to change and improve its business performance.

As mentioned earlier, each ITIM critical process is further broken down into key practices that describe the tasks that an organization should be performing to successfully implement each critical process. Key practices include organizational commitments, which are typically policies and procedures; prerequisites, which are conditions that must exist to implement a critical process successfully; and activities, which address the implementation of policies and procedures.

DHS Has Established the Structure Needed to Effectively Manage Its Investments but Has Yet to Fully Define Many of the Related Policies and Procedures

Through IT investment management, organizations define and follow a corporate process to help senior leadership make informed decisions on competing IT investment options. Such investments, if managed effectively, can have a dramatic impact on an organization's performance and accountability. If mismanaged, they can result in wasteful spending and lost opportunities for improving delivery of services. Based on our framework, an organization should establish the management structure needed to manage its investments; build the investment foundation by selecting and controlling individual projects (Stage 2 capabilities); and manage projects as a portfolio of investments, treating them as an integrated package of competing investment options and pursuing those that best meet the strategic goals, objectives, and mission of the agency (Stage 3 capabilities).

DHS has established the management structure to effectively manage its investments. However, the department has yet to fully define 8 of the 11 related policies and procedures defined by our ITIM framework. Specifically, while DHS has documented the policies and related

[16]40 U.S.C. §§ 11311–11313.

procedures for project-level management, some of these procedures do not include key elements. For example, procedures for selecting investments do not cite either the specific criteria or steps for prioritizing and selecting new IT proposals, and procedures for management oversight of IT projects and systems do not specify the rules that the investment boards are to follow in overseeing investments. In addition, the department has yet to define most of the policies associated with managing its IT projects as investment portfolios. Officials attributed the absence of policies and procedures at the portfolio level to other investment management priorities. Until DHS fully defines and documents its policies and procedures for investment management, it risks selecting investments that will not meet mission needs in the most cost-effective manner.

DHS Has Established an Investment Management Structure and Project-Level Policies, but It Has Not Fully Defined Supporting Procedures

At ITIM Stage 2, an organization has attained repeatable, successful IT project-level investment control processes and basic selection processes. Through these processes, the organization can identify expectation gaps early and take the appropriate steps to address them. ITIM Stage 2 critical processes include (1) defining IT investment board operations, (2) identifying the business needs for each IT investment, (3) developing a basic process for selecting new IT proposals and reselecting ongoing investments, (4) developing project-level investment control processes, and (5) collecting information about existing investments to inform investment management decisions. Table 5 describes the purpose of each of these Stage 2 critical processes.

Table 5: Stage 2 Critical Processes—Building the Investment Foundation

Critical process	Purpose
Instituting the investment board	To define and establish an appropriate IT investment management structure and the processes for selecting, controlling, and evaluating IT investments.
Meeting business needs	To ensure that IT projects and systems support the organization's business needs and meet users' needs.
Selecting an investment	To ensure that a well-defined and disciplined process is used to select new IT proposals and reselect ongoing investments.
Providing investment oversight	To review the progress of IT projects and systems, using predefined criteria and checkpoints, in meeting cost, schedule, risk, and benefit expectations and to take corrective action when these expectations are not being met.
Capturing investment information	To make available to decision makers information to evaluate the impacts and opportunities created by proposed (or continuing) IT investments.

Source: GAO.

DHS has established a management structure within which to execute investment management processes. As previously mentioned, this management structure consists of two review boards, the IRB and the JRC, which are responsible for defining and implementing DHS's IT investment management approach. The membership for these boards appropriately consists of senior executives at the department level and from the major business units and the CIO organization. Other entities, including the EAB and IPRT, play a critical role in supporting the boards and performing investment management activities.

DHS has also fully documented the policies and certain procedures associated with project-level management. Specifically, the department's *Investment Review Process* management directive establishes the framework for department investment management by documenting a high-level investment management process and defining project-level policies, including policies for such key activities as identifying projects or systems that support business needs and selecting among new investment proposals. In addition, other documents specify the procedures associated with these policies. For example, the *Investment Management Handbook* and *Business Case Life Cycle Handbook* specify procedures for relating projects and systems to DHS's business needs, and the *Capital Planning and Investment Control Guide and Systems Development Lifecycle* specify procedures for integrating funding and selection.

Nevertheless, some of DHS's project-level procedures fail to address key elements as follows:

- Procedures for selecting investments do not cite either the specific criteria or steps for prioritizing and selecting new IT proposals. According to officials, such elements are being used to select new IT proposals. However, unless the criteria and steps for prioritizing and selecting new proposals are documented in procedures, it is unlikely that they will be used consistently.

- Procedures for management oversight of IT projects and systems do not specify the steps and criteria (i.e., rules) for the investment boards to follow in controlling investments. Documenting these rules would provide reasonable assurance that key investment control activities are being performed consistently and would establish transparency and thus promote departmentwide understanding of how decisions are made.

- A methodology, with explicit decision-making criteria, does not exist to guide the EAB in determining an investment's alignment with the DHS

enterprise architecture. DHS has developed *Enterprise Architecture Board Process Guidance* that the EAB uses in its reviews of investments,[17] and this guidance contains a standard template for projects to use in providing information to the board; however, it does not describe the procedures governing how alignment is to be determined. As a result, the EAB's assessments are based on subjective and unverifiable judgments. This is a significant weakness given the importance of architecture alignment in ensuring that programs will be defined, designed, and developed in a way that avoids duplication and promotes interoperability and integration.

DHS officials stated that they are aware of the absence of documented procedures in certain areas of project-level management, but said that they are nevertheless carrying out the activities that these procedures would address if they were documented. The officials attributed the absence of procedures to resource constraints, stating that, with a full time staff of six to support departmentwide investment management activities, they are more focused on performing investment management rather than documenting it in great detail. While we do not question the importance of actually implementing IT investment management practices, as evidenced by the fact that our ITIM framework provides for such implementation, it is important to recognize that implementation of undefined processes will at best produce ad hoc and inconsistent results. Accordingly, our framework provides for both documenting how IT investment management is to be performed through policies and procedures and for actually implementing these policies and procedures. Unless DHS's IT investment process guidance specifies procedures for Stage 2 activities that cover all the elements of effective project-level investment management, it is unlikely that key activities will be carried out consistently and in a disciplined manner. This means that DHS is at risk of investing in IT assets that will not cost-effectively meet mission needs.

Table 6 summarizes our findings relative to DHS's execution of the seven key policy and procedure practices needed to manage IT investments at the project level (Stage 2).

[17]The results of the EAB reviews are used as input into the JRC and IRB reviews.

Table 6: Summary of Policies and Procedures for Stage 2 Critical Processes—Building the Investment Foundation

Critical process	Key practice	Rating	Summary of evidence
Instituting the investment board	1. The organization has a documented IT investment process directing each investment board's operations.	Executed	DHS's Investment Review Process management directive and supporting procedural documents define DHS's IT investment process and board operations. These documents generally lay out the roles of the boards and other entities involved in the investment management process, outline significant events and key decision points within the process, and specify the manner in which investment-related processes will be coordinated with other processes, including the strategic planning, budget, and enterprise architecture processes.
Meeting business needs	2. The organization has documented policies and procedures for identifying IT projects or systems that support the organization's ongoing and future business needs.	Executed	DHS's *Investment Review Process* management directive defines the department's policy for ensuring that IT projects and systems support the department's ongoing and future business needs. The supporting procedures are specified in several documents, including the *Investment Management Handbook* and *Business Case Life Cycle Handbook*.
Selecting an investment	3. The organization has documented policies and procedures for selecting new IT proposals.	Not executed	DHS's *Investment Review Process* management directive defines the department's policy for selecting investments. Although supporting procedures exist, they do not specify the criteria and procedures for prioritizing and selecting new IT proposals.
	4. The organization has documented policies and procedures for reselecting ongoing IT investments.	Not executed	DHS's *Investment Review Process* management directive defines the department's policy for reselecting investments. Although supporting procedures exist, they do not specify the criteria and procedures for prioritizing and reselecting ongoing IT investments.
	5. The organization has policies and procedures for integrating funding with the process of selecting an investment.	Executed	DHS's *Investment Review Process* management directive, *Capital Planning and Investment Control Guide*, and *Systems Development Lifecycle* specify policies and procedures for integrating funding with the process of selecting an investment.
Providing investment oversight	6. The organization has documented policies and procedures for management oversight of IT projects and systems.	Not executed	DHS's *Investment Review Process* management directive sets the policy for management oversight of IT projects and systems. The supporting procedures, however, are lacking key elements, including the procedural rules for the investment boards operations and decision making during project oversight.
Capturing investment information	7. The organization has documented policies and procedures for identifying and collecting information about IT projects and systems to support the investment management process.	Not executed	Although DHS policy documents the types of information to be collected about IT projects and systems to support the investment management process, the department does not have supporting procedures that explicitly assign responsibility and ownership of information or define the physical and logical locations for information storage.

Source: GAO analysis of DHS data.

DHS Has Largely Not Documented Policies and Procedures for Portfolio Management

Once an agency has attained Stage 2 (i.e., project-level) maturity, it needs to effectively manage critical processes for managing its investments as a portfolio or set of portfolios (Stage 3). IT investment portfolios are integrated, agencywide collections of investments that are assessed and managed collectively based on common criteria. Managing investments as portfolios is a conscious, continuous, and proactive approach to allocating limited resources among an organization's competing initiatives in light of the relative benefits expected from these investments. Taking an agencywide perspective enables an organization to consider its investments in a more comprehensive and integrated fashion, so that collectively the investments optimally address the organization's missions, strategic goals, and objectives. Managing IT investments as portfolios also allows an organization to determine its priorities and make decisions about which projects to begin funding and continue to fund based on analyses of the relative organizational value and risks of all projects, including projects that are proposed, under development, and in operation. Although investments may initially be organized into subordinate portfolios—based on, for example, business lines or life cycle stages—and managed by subordinate investment boards, they should ultimately be aggregated into enterprise-level portfolios.

According to ITIM, Stage 3 maturity involves (1) defining the portfolio criteria; (2) creating the portfolio; (3) evaluating (i.e., overseeing) the portfolio; and (4) conducting PIRs. Table 7 summarizes the purpose of each of these processes.

Table 7: Stage 3 Critical Processes—Developing a Complete Investment Portfolio

Critical process	Purpose
Defining the portfolio criteria	To ensure that the organization develops and maintains IT portfolio selection criteria that support its mission, organizational strategies, and business priorities.
Creating the portfolio	To ensure that IT investments are analyzed according to the organization's portfolio selection criteria and to ensure that an optimal IT investment portfolio with manageable risks and returns is selected and funded.
Evaluating the portfolio	To review the performance of the organization's investment portfolio(s) at agreed-upon intervals and to adjust the allocation of resources among investments as necessary.
Conducting postimplementation reviews	To compare the results of recently implemented investments with the expectations that were set for them and to develop a set of lessons learned from these reviews.

Source: GAO.

DHS has not yet fully established any of the policies and procedures associated with managing the 22 IT portfolios that it recently established. For example, the department does not have documented policies and procedures for creating and modifying portfolio selection criteria or for

creating its portfolios. In addition, DHS does not have documented policies and procedures for evaluating (or controlling) its portfolios. Further, while the department has policies and procedures for conducting PIRs, these policies and procedures do not specify several items, including roles and responsibilities for conducting reviews, and how conclusions, lessons learned, and recommended management actions are to be shared with executives and others.

DHS officials attributed the lack of portfolio-level policies and procedures to the fact that resources have been assigned to other investment management activities, such as its efforts to establish the 22 portfolios. However, they said that establishing these policies and procedures is important, and thus they are taking steps to begin defining them. Specifically, they said that a portfolio manager for four portfolios—Grants, Case Management, Portal, and Disaster Management—was hired in the fall of 2006, and this manager's responsibilities include developing the direction, guidance, and procedures for departmental portfolio management. They also said that another portfolio manager is currently being recruited. In addition, DHS officials stated that the PIR procedures defined in the *Operational Analysis Guide* are being updated to focus more on lessons learned.

Not having documented policies and procedures for portfolio management is a significant weakness, particularly since officials told us that they recently began performing control reviews of these portfolios. Until DHS fully establishes the policies and procedures for portfolio-level management, DHS is at risk of not selecting and controlling the mix of investments in a manner that best supports the department's mission needs.

As illustrated in table 10, none of the practices associated with policies and procedures for Stage 3 have been executed. Table 8 summarizes the rating for each critical process required to manage investments as a portfolio and summarizes the evidence that supports these ratings.

Table 8: Summary of Policies and Procedures for Stage 3 Critical Processes—Developing a Complete Investment Portfolio

Critical process	Key practice	Rating	Summary of evidence
Defining the portfolio criteria	The organization has documented policies and procedures for creating and modifying IT portfolio selection criteria.	Not executed	While DHS recently developed and vetted its IT portfolios, it has not documented policies and procedures for creating and modifying the portfolio selection criteria.
Creating the portfolio	The organization has documented policies and procedures for analyzing, selecting, and maintaining the investment portfolio(s).	Not executed	DHS does not have policies and procedures for analyzing, selecting, and maintaining its investment portfolios.
Evaluating the portfolio	The organization has documented policies and procedures for reviewing, evaluating, and improving the performance of its portfolio(s).	Not executed	DHS does not have documented policies and procedures for reviewing, evaluating, and improving the performance of its portfolios, although officials told us that the department has recently begun to perform portfolio reviews.
Conducting postimplementation reviews	The organization has documented policies and procedures for conducting PIRs.	Not executed	Although DHS has policies and procedures for conducting PIRs, they do not specify key items, including roles and responsibilities for conducting PIRs.

Source: GAO.

DHS Has Not Fully Executed Key Practices Associated with Effectively Controlling Investments

DHS has not fully implemented any of the key practices needed to control investments—either at the project level or at the portfolio level. For example, according to DHS officials and our review of the department's control review schedule, the investment boards have not conducted regular reviews of investments. Further, while control activities are sometimes performed, they are not performed consistently across projects. In addition, because the policies and procedures for portfolio management have yet to be defined, control of the department's investment portfolios is ad hoc, according to DHS officials. Officials told us that to strengthen IT investment management, they have recently hired a portfolio manager and are recruiting another one. Until DHS fully implements processes to control its investments, both at the project and portfolio levels, it increases the risk of not meeting cost, schedule, benefit, and risk expectations.

DHS Has Not Implemented the Key Practices Associated with Controlling Investments at the Project Level

As we have previously reported, an organization should effectively control its IT projects throughout all phases of their life cycles. In particular, its investment board should observe each project's performance and progress toward predefined cost and schedule expectations, as well as each project's anticipated benefits and risk exposure. The board should also employ early warning systems that enable it to take corrective actions when cost, schedule, and performance expectations are not met.

According to our ITIM framework, effective project-level control[18] requires, among other things, (1) providing adequate resources for IT project oversight; (2) developing and maintaining an approved management plan for each IT project; (3) making up-to-date cost and schedule data for each project available to the oversight boards; (4) having regular reviews by each investment board of each project's performance against stated expectations; and (5) ensuring that corrective actions for each underperforming project are documented, agreed to, implemented, and tracked until the desired outcome is achieved. (The key practices are listed in table 9.)

Although (as discussed in the previous section), DHS has established some policies and procedures, DHS has not implemented any of the prerequisites and activities associated with effective project control. For example, DHS officials stated that the department does not have adequate resources, including human capital, for project oversight.

In addition, although DHS policies and procedures call for certain control activities to be performed, these have not always taken place. For example, DHS policy and procedures call for cost, schedule, benefit, and risk parameters to be documented in (1) Acquisition Program Baselines (APB) and risk management plans for major projects in the *capability development and demonstration or production and deployment* phases and (2) in operational analysis (OA) documents and Exhibit 300s for projects in operations and support (steady state). However, DHS officials acknowledged that some projects do not have APBs or OAs and stated that a management directive to implement the OA policy is in draft. In addition, although the APBs are supposed to be approved by the appropriate board at the *alternative selection* milestone decision point, DHS officials stated that this does not always happen. Instead, these officials said that the Office of Program Analysis and Evaluation is reviewing APBs for "interim approval." In addition, OAs are currently reviewed by the boards only if a

[18]In our ITM framework, project-level control is associated with the Stage 2 critical process *Providing Investment Oversight.*

problem arises with the projects. Of the three investments we reviewed,[19] an APB and risk management plan were developed for one (Transportation Worker Identification Credentialing or TWIC). However, these documents are being updated to reflect changes in the project's scope and have not yet been approved by the IRB. For another investment (Integrated Wireless Network or IWN), although, according to officials, an APB was developed, it was not approved by the IRB, although it should have been given its life cycle stage. For the third investment (National Emergency Management Information System or eNEMIS), an OA document specifies the cost, schedule, and benefit expectations for the project. However, the OA has not been reviewed by an investment board because the project has not experienced a problem that would trigger its review.

Data on actual performance are also not provided to the appropriate IT investment board on a regular basis. Specifically, according to the *Investment Review Process* management directive, *Periodic Reporting Manual*, *and Investment Management Handbook*, actual cost, schedule, and benefits performance data for projects through the *production and deployment* phase should be provided to the boards in the APB and the IPRT's analyses of quarterly reports for key milestone decision reviews and annual reviews. However, our review of the fiscal year 2006 control schedule showed that project reviews did not always occur; therefore, the boards were not provided with data on actual project performance on a regular basis. In addition, a schedule for fiscal year 2007 project reviews has not been developed. Moreover, officials confirmed that these reviews do not always occur stating that, for fiscal year 2007, the boards' reviews have been scheduled reactively, for projects that have legislatively required expenditure plans or have otherwise prompted congressional interest. In addition, while the IPRT is supposed to monitor data on the actual performance of projects in operations and support, these data are provided to the boards only if problems arise.

[19]We reviewed three investments as part of our evaluation—TWIC (Transportation Worker Identification Credentialing), which is intended to improve security by establishing a systemwide common secure credential, used across all transportation nodes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system; IWN (Integrated Wireless Network), which is to provide a coordinated nationwide approach to reliable, seamless, interoperable wireless communications; and eNEMIS (National Emergency Management Information System), which is a mission critical application and infrastructure that supports the entire life cycle of emergency or disaster (including acts of terrorism) declarations. These projects are described in greater detail in appendix I.

Regarding investment board reviews of the performance of IT projects and systems against expectations, DHS's policy requires that ongoing project reviews be conducted either annually or at milestone decision points. However, these reviews are not conducted in a timely manner for all level 1 and 2 investments that are not the subject of congressional interest. Officials stated that the Under Secretary for Management would likely be issuing new guidance aimed at making the review schedule more proactive.

Finally, DHS officials told us that the investment boards do not effectively track the implementation of corrective actions for underperforming projects, primarily because they do not have a robust tool to support them in this activity.

This means that DHS executives do not have the information they need to determine whether investments are meeting expectations, which increases the risk that underperforming projects will not be identified and corrected in a timely manner.

Table 9 shows the ratings for each key practice required to control investments (except for the policies and procedures, which were discussed in the previous section) and summarizes the evidence that supports these ratings.

Table 9: Summary of Key Practices for Providing Investment Oversight (Stage 2 Critical Process)

Type of practice	Key practice	Rating	Summary of evidence
Prerequisite	Adequate resources, including people, funding, and tools, are provided for IT project oversight.	Not executed	According to DHS officials, the department does not have adequate resources for project oversight. Specifically, staff resources fall short of the required number and experience level. In addition, officials stated that the board does not have a robust tool to track the implementation of corrective actions for underperforming projects.
Prerequisite	IT projects and systems, including those in steady state (operations and maintenance), maintain approved project management plans that include expected cost and schedule milestones and measurable benefit and risk expectations.	Not executed	DHS's *Investment Review Process* management directive and supporting procedures specify that all major projects in the *capability development and demonstration* phase or in the *production and deployment* phase of the life cycle should have an APB that defines the projects' cost, schedule, and performance parameters and a risk management plan that identifies expected risks. They also specify that the APB and risk management plan should be approved by the appropriate board at key milestone decision points. However, DHS officials told us that not all investments have an APB. They also stated that, for those that have APBs, these documents are not always approved by the boards. In addition, officials stated that all major projects in steady state are to have an OA that documents expected cost, schedule, and benefit parameters. However, DHS officials stated that not all operational programs currently have OAs. Risk factors for steady state projects are addressed in Exhibit 300s. None of the three investments we reviewed (TWIC, IWN, and eNEMIS) satisfied this key practice. Specifically, for TWIC, an APB and risk management plan were developed, but these documents are being updated to reflect changes in the project's scope and have not yet been approved by the IRB. For IWN, according to officials, an APB has been prepared, but it has not been approved by the IRB, although it should have been, given its life cycle stage. For eNEMIS, a June 2006 OA document was prepared, but it has not been approved by the review board. According to officials, such approval of the OA document is not required.

Type of practice	Key practice	Rating	Summary of evidence
Activity	Data on actual performance (including cost, schedule, benefit, and risk performance) are provided to the appropriate IT investment board.	Not executed	According to the I*nvestment Review Process* management directive, *Periodic Reporting Manual*, and *Investment Management Handbook*, actual cost, schedule, and benefits performance data for projects through the *production and deployment* phase should be provided to the boards in the APB and the IPRT's analyses of quarterly reports for key milestone decision reviews and annual reviews. However, according to our review of the control schedule and DHS officials, this is not happening in some cases. In addition, while the IPRT is to monitor data on the actual performance of projects that are the in *operations and support* phase, these data are provided to the boards only if problems arise. Of the three investments that we reviewed, TWIC satisfied this key practice since actual performance data for TWIC was last presented to the IRB for a key milestone decision review in March 2006. However, IWN and eNEMIS did not satisfy this key practice. Specifically, we received the quarterly report for IWN containing data on actual performance but received no evidence that the data were provided to the board. Because eNEMIS is a steady state investment, it was not required to submit data on actual performance to the investment board.
Activity	Using verified data, each investment board regularly reviews the performance of IT projects and systems against stated expectations.	Not executed	According to DHS officials, the IPRT verifies data on the performance of IT investments against stated expectations and provides summaries and analyses of verified data to the boards for their milestone decision reviews and annual reviews. However, the department's control schedule shows that the boards have not conducted regular reviews of investments. Instead, officials told us that the boards have reacted to projects that are the focus of congressional interest. Moreover, steady state investments are not reviewed by upper management review boards (the IRB or JRC) unless the analysis conducted for the initial review by the IPRT indicates a problem. Of the three investments that we reviewed, TWIC is the only project that satisfied this key practice. Specifically, TWIC's performance against expectations was reviewed by the IRB. Implementation plans for IWN are currently being revised and, according to officials, are to be reviewed by the IRB in April 2007. As noted earlier, eNEMIS was not reviewed by a board since it is a steady state project.
Activity	For each underperforming IT project or system, appropriate actions are taken to correct or terminate the project or system in accordance with defined criteria and the documented policies and procedures for management oversight.	Not executed	According to DHS's *Periodic Reporting Manual*, projects in the *capability development and demonstration* or *production and deployment* phases are to report on projects whose cost, schedule, and performance variances exceed the investment's APB by 8 percent (plus or minus) on a quarterly basis and to submit a remediation plan within 30 days. Of the three investments that we reviewed, officials told us that TWIC was the only investment that experienced performance shortfalls. However, according to officials, a remediation plan documenting the corrective actions for this investment was not prepared. As previously noted, the department does not have policies and procedures for ensuring that appropriate actions are taken for underperforming steady state projects.

Type of practice	Key practice	Rating	Summary of evidence
Activity	The investment board regularly tracks the implementation of corrective actions for each underperforming project until the actions are completed.	Not executed	The CFO Planning Analysis and Evaluation and CIO Enterprise Business Management officials stated that although there is a tool in place to track corrective actions, it is not yet shared across the IPRT and needs improvement.

Source: GAO.

DHS Has Not Implemented Key Practices Needed to Control Its Investment Portfolios

The critical process associated with controlling investment portfolios (*evaluating the portfolio* under Stage 3 of our ITIM framework) builds upon the Stage 2 critical process *providing investment oversight* by adding the elements of portfolio performance to an organization's investment control capacity. Compared with less mature organizations, Stage 3 organizations will have the capability to control the risks faced by each investment and to deliver benefits that are linked to mission performance. In addition, a Stage 3 organization will have the benefit of performance data generated by Stage 2 processes. Executive-level oversight of risk management outcomes and incremental benefit accumulation provides the organization with increased assurance that each IT investment will achieve the desired results. Table 10 lists the key practices associated with this critical process, with the exception of the establishment of policies and procedures, which was discussed earlier.

Table 10: Summary of Key Practices for Evaluating the Portfolio (Stage 3 Critical Process)

Type of practice	Key practice
Prerequisites	Adequate resources, including people, funding, and tools have been provided for reviewing the investment portfolio and its projects.
	Board members are familiar with the process for evaluating and improving the portfolio's performance.
	Results of relevant providing investment oversight reviews from Stage 2 are provided to the investment board.
	Criteria for assessing portfolio performance are developed, reviewed, and modified at regular intervals to reflect current performance expectations.
Activities	IT portfolio performance measurement data are defined and collected consistent with portfolio performance criteria.
	Adjustments to the IT investment portfolio are executed in response to actual portfolio performance.

Source: GAO.

Although officials told us that DHS has taken steps to classify its investments into 22 IT portfolios, the department has largely not defined the policies and procedures needed to control these portfolios (see earlier section of this report). As a result, DHS officials stated that they are performing portfolio-level control in an ad hoc manner. To begin addressing this, they stated that an analyst was recently hired to help develop guidance and procedures for the IT portfolios, and another staff member is being recruited. Without documented policies and procedures for controlling its investment portfolios, the department's efforts to evaluate its portfolios will remain ad hoc, compounding its risk of investing in new and existing IT systems that are not aligned with DHS's mission and business priorities and do not meet cost, schedule, and performance expectations.

Conclusions

Given the importance of IT to DHS's mission performance and outcomes, it is vital for the department to adopt and employ an effective institutional approach to IT investment management. To its credit, the department has established aspects of such an approach and thus has a basis for achieving greater maturity. However, its approach is missing key elements of effective investment management, such as procedures for implementing project-specific investment management policies, as well as policies and procedures for portfolio-based investment management. Further, it has yet to fully implement either project- or portfolio-level investment control practices. All told, this means that DHS lacks the complete institutional capability needed to ensure that it is investing in IT projects that best support its strategic mission needs and that ongoing projects will meet cost, schedule, and performance expectations. After almost 4 years in operation, DHS is overdue in having a mature approach to investment management. Without one, DHS is impaired in its ability to optimize mission performance and accountability.

Recommendations for Executive Action

To strengthen DHS's investment management capability and address the weaknesses discussed in this report, we recommend that the Secretary of Homeland Security direct the Undersecretary for Management, in collaboration with the CFO and CIO, to devote the appropriate attention to development and implementation of effective investment management processes. At a minimum, this should include fully defining and documenting project-and portfolio-level policies and procedures that address the following eight areas:

- selecting new investments, including specifying the criteria and steps for prioritizing and selecting these proposals;
- reselecting ongoing IT investments, including specifying the criteria and steps for prioritizing and reselecting these investments;
- overseeing (i.e., controlling) IT projects and systems, including specifying the procedural rules for the investment boards' operations and decision making during project oversight;
- identifying and collecting information about investments, including assigning responsibility for the process and ownership of the information and defining the locations for information storage;
- creating and modifying IT portfolio selection criteria;
- analyzing, selecting, and maintaining the investment portfolios;
- assessing portfolio performance at regular intervals to reflect current performance expectations; and
- conducting postimplementation reviews of IT investments, including defining roles and responsibilities for doing so, and specifying how conclusions, lesson learned, and recommended management actions are to be shared with executives and others.

In addition, we recommend that the department implement key investment control processes. At a minimum, this should include these six project-level practices:

- providing adequate resources, including people, funding, and tools, for IT project oversight;
- having IT projects and systems, including those in steady state (operations and maintenance), maintain approved project management plans that include expected cost and schedule milestones and measurable benefit and risk expectations;
- providing data on actual performance (including cost, schedule, benefit, and risk performance) to the appropriate IT investment board;
- having each investment board use verified data to regularly review the performance of IT projects and systems against stated expectations;

- taking appropriate actions to correct or terminate each underperforming IT project or system in accordance with defined criteria and the documented policies and procedures for management oversight; and
- having the investment board regularly track the implementation of corrective actions for each underperforming project until the actions are completed.

It should also include the following six portfolio-level practices:

- providing adequate resources, including people, funding, and tools, for reviewing the investment portfolios and their projects;
- making board members familiar with the process for evaluating and improving the portfolio's performance;
- providing results of relevant *Providing Investment Oversight* reviews from Stage 2 to the investment boards;
- developing, reviewing, and modifying criteria for assessing portfolio performance at regular intervals to reflect current performance expectations;
- defining and collecting IT portfolio performance measurement data that are consistent with portfolio performance criteria; and
- executing adjustments to the IT investment portfolios in response to actual portfolio performance.

Agency Comments

In DHS's written comments on a draft of this report, signed by the Director, Departmental GAO/Office of Inspector General Liaison, the department stated that it agreed with our findings and recommendations and will use the report to improve its investment management and review processes. The department's written comments are reprinted in appendix II. The department also provided technical comments that we incorporated in the report where appropriate.

We are sending copies of this report to the Chairmen and Ranking Minority Members of other Senate and House committees that have authorization and oversight responsibilities for homeland security and other interested congressional committees; the Director of the Office of Management and Budget; and the DHS Secretary, Undersecretary for

Management, Chief Financial Officer, and Chief Information Officer. We also will make copies available to others upon request. In addition, the report will be made available at no charge on the GAO Web site at www.gao.gov.

If you or your staff have any questions about matters discussed in this report, please contact me at (202) 512-3439 or by e-mail at hiter@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs Office may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) determine whether the Department of Homeland Security (DHS) has established the management structure and policies and procedures needed to effectively manage its information technology (IT) investments and (2) determine whether the department is implementing key practices needed to effectively control these investments.

To address our first objective, we reviewed the results of the department's self-assessment of practices associated with project-level and portfolio-level policies and procedures and compared them against the relevant practices in Stages 2 and 3 of our IT Investment Management (ITIM) framework. We also validated and updated the results of the self-assessment through document reviews and interviews with officials. We reviewed written policies, procedures, guidance, and other documentation providing evidence of executed practices, including DHS's *Investment Review Process Management Directive*, *Capital Planning and Investment Control Guide*, *Investment Management Handbook*, *Periodic Reporting Manual*, and various management memoranda. Our review focused on DHS's capabilities related to Stages 2 and 3 in our framework that relate to policies and procedures because those stages lay the foundation for higher maturity stages and assist organizations in complying with the investment management provisions of the Clinger Cohen Act.

To address our second objective, we reviewed the results of the department's self-assessment of critical processes within Stages 2 and 3 that are associated with project-level and portfolio-level oversight and compared them against our ITIM framework. We also validated and updated the results of the self-assessment through document reviews and interviews with officials. In addition, we reviewed DHS's Investment Review Board, Joint Resources Council, and Enterprise Architecture Board investment-related materials, including the investment review boards' control schedule, status reports, meeting minutes, portfolio-related documents, and records of decisions. We also conducted interviews with officials from the Office of the Chief Information Officer, the Office of the Chief Financial Officer, and the Office of Program Analysis and Evaluation whose main responsibilities are to control investments and ensure that DHS's IT investment management process is implemented and followed.

As part of our analysis for the second objective, we selected three investments as case studies to verify that the key practices for investment control were being applied. The investments selected were major systems when we began our review. They also (1) represented a mix of

enterprisewide (i.e., headquarters) and component agency investments; and (2) spanned different life cycle phases. The three investments are described below:

- DHS Integrated Wireless Network (IWN)—This network is to provide a coordinated nationwide approach to reliable, seamless, interoperable wireless communications. It is intended to support federal agents and officers engaged in the conduct of law enforcement, protective services, homeland defense, and disaster response with DHS, the Department of Justice, and the Department of the Treasury. IWN is a major enterprisewide investment and is in the *capability development and demonstration* phase. It has an estimated life cycle cost of $4.3 billion and is designated as a level 1 investment.

- Transportation Security Administration's Transportation Worker Identification Credentialing (TWIC)—This project is intended to improve security by establishing a systemwide common secure credential, used across all transportation nodes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system. It is a major component agency investment and is designated as a level 1 investment. The total cost of the program is estimated at appropriately $307 million through fiscal year 2012.

- Federal Emergency Management Agency's National Emergency Management Information System (eNEMIS)—eNEMIS is a mission critical application and infrastructure that supports the entire life cycle of emergency or disaster (including acts of terrorism) declarations. The project tracks major incidents; supports mission assignments and other predeclaration response activities; processes the governor's request for assistance; and automates the preliminary damage assessment process, the regional analysis, and summary. It is a major component agency investment that is in the operations and support phase and is designated as a level 1 investment with an estimated total life cycle cost of $319 million.

For these investments, we reviewed project management documentation, such as acquisition program baseline, operational analysis document, and decision memoranda.

For both objectives, we rated the ITIM key practices as "executed" on the basis of whether the agency demonstrated (by providing evidence of performance) that it had fully met the criteria of the key practice. A key practice was rated as "not executed" when we found insufficient evidence of a practice during the review or when we determined that there were significant weaknesses in DHS's execution of the key practice. We

provided DHS an opportunity to produce evidence for the key practices that we rated as "not executed."

We conducted our work at DHS headquarters in Washington, D.C., from February 2006 through March 2007 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the U.S. Department of Homeland Security

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

Homeland Security

April 16, 2007

Mr. Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hite:

RE: Draft Report GAO-07-424, Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments (GAO Job Code 310617)

The Department of Homeland Security appreciates the opportunity to review and comment on the draft report referenced above. The Government Accountability Office makes two broad recommendations: (1) devote appropriate attention to the development and implementation of effective management processes and (2) implement key investment control processes.

We agree with the findings and recommendations and will use the report findings to improve the Department's investment-management and investment-review procedures. Management Directive 0007.1, signed by the Secretary, solidifies the primary role of the Chief Information Officer functions within the Department, provides for a review of all IT budgets within the Department, and provides the format for the Chief Information Officer approval of component information technology budgets and information technology procurements greater than $2.5 million.

Technical comments that update or clarify statements in the draft report are provided under separate cover.

Sincerely,

Steven J. Pecinovsky

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

www.dhs.gov

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439, or hiter@gao.gov

Staff Acknowledgments

In addition to the individual named above, Sabine Paul, Assistant Director; Gary Mountjoy, Assistant Director; Mathew Bader; Justin Booth; Barbara Collier; Tomas Ramirez; and Niti Tandon made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER