United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2012

INFORMATION TECHNOLOGY

DHS Needs to Further Define and Implement Its New Governance Process

GAO-12-818

July 2012

INFORMATION TECHNOLOGY

DHS Needs to Further Define and Implement Its New Governance Process

GAO Highlights

Accountability * Integrity * Reliability

Highlights of GAO-12-818, a report to congressional requesters

Why GAO Did This Study

DHS has one of the largest IT budgets in the federal government. In fiscal year 2012, DHS plans to spend about $5.6 billion to, among other things, acquire, implement, and operate approximately 360 IT programs, including about 83 major programs, which are intended to assist in carrying out its diverse missions. With such a large portfolio of IT programs, it is important to ensure that the appropriate governance exists so that the programs meet their cost, schedule, and performance goals and continue to support the department's strategies and objectives. In line with this, DHS has been working to define and implement a new IT governance process.

GAO was asked to (1) describe DHS's new IT governance process and associated policies and procedures, and assess them against best practices; and (2) determine progress made in implementing the new process and how DHS's implementation efforts comport with relevant best practices. To do so, GAO analyzed relevant documentation and interviewed DHS officials responsible for defining and implementing the new governance process.

What GAO Recommends

To implement an effective IT governance process, GAO recommends that DHS finalize associated policies and procedures, and fully follow best practices for implementing the process. In comments on a draft of this report, DHS concurred with GAO's recommendations and estimated it would address them by September 2013.

View GAO-12-818. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has defined a vision for its new information technology (IT) governance process, which includes a tiered oversight structure that defines distinct roles and responsibilities throughout the department. The new governance framework and the associated policies and procedures are generally consistent with recent Office of Management and Budget (OMB) guidance and with best practices for managing projects and portfolios identified in GAO's IT Investment Management framework, with two practices partially addressed and seven others fully addressed. For example, consistent with OMB guidance calling for the Chief Information Officer (CIO) to play a significant role in overseeing programs, DHS's draft procedures require that lower-level boards overseeing IT programs include the DHS CIO, a component CIO, or a designated executive representative from a CIO office. In addition, consistent with practices identified in GAO's IT Investment Management framework, DHS's draft procedures identify key performance indicators for gauging portfolio performance. However, DHS's policies and procedures have not yet been finalized, because, according to officials, the focus has been on piloting the new governance process. While it is important to conduct pilots to test processes and identify lessons learned, until the department finalizes the policies and procedures associated with the new IT governance, it will have less assurance that its new IT governance will be consistent with best practices and address previously identified weaknesses in investment management.

DHS has begun to implement aspects of its new governance process. For example, it has established several governance entities and conducted program health assessment reviews for all of its major IT programs. In implementing its new governance, the department has generally followed key industry best practices, such as establishing an implementation team; however, the department has not fully followed other practices, including developing a mechanism to capture lessons learned. The table below summarizes GAO's assessment of DHS's implementation efforts. Until the department fully addresses these practices, its implementation approach may be less effective than intended.

Assessment of DHS's Implementation Efforts

Best practice	DHS's implementation efforts
Organizational buy-in	DHS has organizational buy-in from top management, as evidenced by the Under Secretary for Management approving key documents supporting the new IT governance process. In addition, the Office of the CIO took steps to secure stakeholder buy-in.
Implementation team and plan	DHS has established a team for implementing its IT governance structure; however, the department has not yet developed an implementation plan.
Evaluation	DHS has documented several performance measures, including measures to assess the effectiveness of Executive Steering Committee meetings, but has not documented others. In addition, DHS does not have mechanisms to capture lessons learned.

Source: GAO analysis of DHS data.

Contents

Abbreviations

CIO	chief information officer
COE	Centers of Excellence
DHS	Department of Homeland Security
EBMO	Enterprise Business Management Office
ESC	Executive Steering Committee
IRB	Investment Review Board
IT	information technology
ITIM	Information Technology Investment Management
OMB	Office of Management and Budget
PARM	Program Accountability and Risk Management

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 25, 2012

The Honorable Tom Carper
Chairman
Subcommittee on Federal Financial Management,
Government Information, Federal Services,
and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael T. McCaul
Chairman
The Honorable William R. Keating
Ranking Member
Subcommittee on Oversight, Investigations,
and Management
Committee on Homeland Security
House of Representatives

The Department of Homeland Security (DHS) has one of the largest information technology (IT) budgets in the federal government. With a fiscal year 2012 IT budget of about $5.6 billion, DHS plans to use these funds to, among other things, acquire, implement, and operate approximately 360 IT programs, including about 83 major[1] programs, to assist in carrying out its diverse missions. Given the size of DHS's IT portfolio and its importance to the department's mission, it is important to ensure that the appropriate governance exists so that the programs meet their cost, schedule, and performance goals and continue to support the department's strategies and objectives. According to the IT Governance Institute's *Control Objectives for Information and related Technology 4.1*,[2] IT governance is the responsibility of executives, and consists of the leadership, organizational structures, and processes that ensure that an

[1]DHS defines major IT acquisitions as those having life cycle cost estimates of $50 million or more.

[2]IT Governance Institute, *Control Objectives for Information and related Technology 4.1* (Rolling Meadows, Ill.: 2007).

enterprise's IT sustains and extends the organization's strategies and objectives.[3]

In 2003, we designated implementing and transforming DHS as high risk, in part due to weaknesses related to the department's management of its IT programs.[4] In 2011, the department introduced a new initiative to improve and streamline its IT governance and address continuing weaknesses. This report responds to your request that we conduct a review of DHS's new IT governance process. Specifically, our objectives were to (1) describe DHS's new IT governance process and associated policies and procedures, and assess them against best practices; and (2) determine progress made in implementing the new process and how DHS's implementation efforts comport with relevant best practices.

To address these objectives, we analyzed documents such as the DHS Under Secretary for Management's *Program Management & Execution Playbook, the Integrated Strategy for High Risk Management Implementation and Transformation*, and Chief Information Officer's (CIO) draft Concept of Operations documents for Program Governance and Portfolio Governance. We also interviewed officials from DHS's Office of the CIO's Enterprise Business Management Office (EBMO) who have primary responsibility for defining and implementing the new governance process, and from the Office of Program Accountability and Risk Management (PARM) who have general responsibility for acquisition management policy. We assessed the governance framework against GAO's Information Technology Investment Management (ITIM) guide,[5]

[3]According to the IT Governance Institute, IT governance is also the responsibility of the board of directors. However, we have omitted that reference because it is not relevant to DHS.

[4]GAO, *High-Risk Series: An Update,* GAO-11-278 (Washington, D.C.: February 2011). GAO designated implementing and transforming DHS as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. The high-risk area includes challenges in strengthening DHS's management functions, including acquisition, IT (which included IT governance), financial, and human capital management; the impact of those challenges on DHS's mission implementation; and challenges in integrating management functions within and across the department and its components.

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

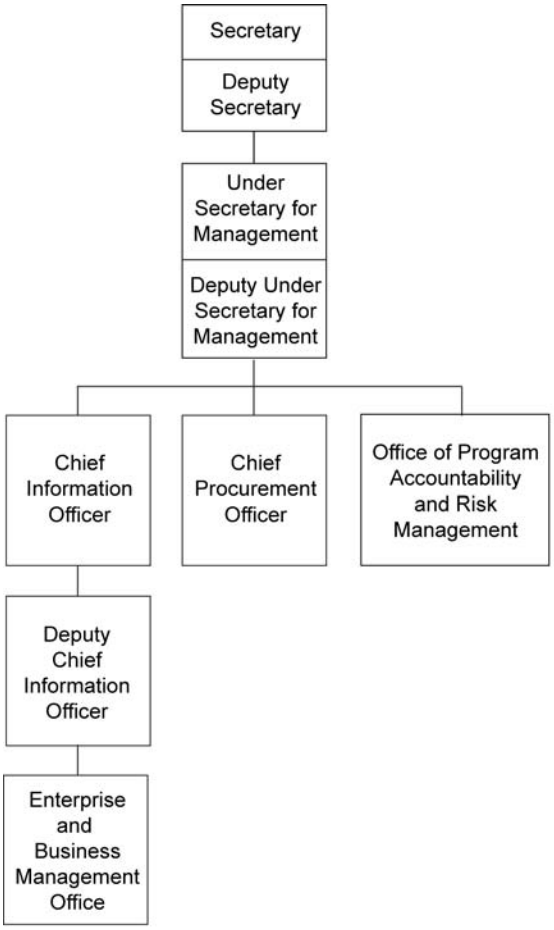
and the implementation of the framework against industry best practices. Details on our scope and methodology can be found in appendix I.

We conducted this performance audit from October 2011 to July 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DHS's mission is to lead 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. The department is also responsible for ensuring that the nation's borders are safe and secure, welcoming lawful immigrants and visitors, and promoting the free flow of commerce. Created in 2002, DHS assumed control of about 209,000 civilian and military positions from 22 agencies and offices that specialize in one or more aspects of homeland security. The intent behind the merger that created DHS was to improve coordination, communication, and information sharing among these multiple federal agencies. Each of these agencies is responsible for specific homeland security missions and for coordinating related efforts with its sibling components, as well as external entities. Figure 1 shows the department-level organizations which are responsible for or share responsibility for IT acquisition management activities.

Figure 1: DHS Department-level Organizations with IT Acquisition Management Responsibilities



Source: GAO analysis of DHS data.

Within the department's Management Directorate, headed by the Under Secretary for Management, is the Office of the CIO. The CIO's responsibilities include setting departmental IT policies, processes, and standards, and ensuring that IT acquisitions comply with DHS IT management processes, technical requirements, and approved enterprise architecture, among other things. Additionally, the CIO chairs DHS's Chief Information Officer Council, which is responsible for ensuring the development of IT resource management policies, processes, best practices, performance measures, and decision criteria for managing the delivery of IT services and investments, while controlling costs and mitigating risks.

Within the Office of the CIO, EBMO has been given primary responsibility for ensuring that the department's IT investments align with its missions and objectives. EBMO was recently reorganized to include a new Enterprise Portfolio Governance Division dedicated to executing portfolio reviews. This division is to provide support to portfolio stakeholders to administer portfolio activities, such as aligning programs with portfolios, creating baseline portfolios, and establishing portfolio pilot efforts.

In October 2011, DHS realigned its acquisition management functions previously performed by divisions within the Office of the Chief Procurement Officer to establish PARM.[6] The office, which reports directly to the Under Secretary for Management, is to ensure the effectiveness of the overall program execution governance process in support of the department's Investment Review Board (IRB), and has the responsibility for developing and maintaining DHS's *Acquisition Management Directive*.[7] PARM is also responsible for providing independent assessments of major investment programs, and monitoring programs between formal reviews to identify any emerging issues that DHS needs to address to keep the programs on track.

DHS's Acquisition Management Process

DHS acquisitions—which are expected to total about $18 billion in fiscal year 2012—support a wide range of missions and investments, including ships and aircraft, border surveillance and screening equipment, nuclear detection equipment, and systems to track the department's financial and human resources. In support of its diverse missions, DHS plans to spend about $5.6 billion in fiscal year 2012 to deploy and maintain over 360 IT programs to perform both mission-critical and support functions, which frequently must be coordinated among components, as well as among external entities. In 2003, DHS established an investment review process to help reduce risk and increase the chances for successful acquisition outcomes by providing departmental oversight of major investments throughout their life cycle and to help ensure that funds allocated for investments through the budget process are being spent wisely,

[6]PARM incorporates the functions and responsibilities previously performed by the Acquisition Program Management Division and the Cost Analysis Division of the Office of the Chief Procurement Officer.

[7]Department of Homeland Security, *Acquisition Management Directive, Directive Number 102-01* (Jan. 20, 2010). Guides supporting this directive were updated in October 2011.

efficiently, and effectively. In October 2010, DHS updated the acquisition guidance, which outlined the acquisition life cycle phases and called for senior-level approval of each major acquisition program at key decision events during a program's acquisition life cycle.

DHS's Acquisition Review Board —renamed the IRB in October 2011— was established to review and approve major acquisition programs,[8] at key stages in their life cycles before the acquisition program could move to the next phase.[9] DHS's guidance establishes four phases that constitute the acquisition life cycle:

1. The need phase—during which a problem is defined and the needed capability is identified. This phase concludes with the IRB granting the acquisition program approval to proceed at Acquisition Decision Event 1.

2. The analyze/select phase—during which it is determined how to provide the needed capability. This phase concludes with the IRB granting the acquisition program approval to proceed at Acquisition Decision Event 2A.

3. The obtain phase—during which the needed capability is obtained. The IRB may review the acquisition program multiple times before granting the acquisition program approval to proceed with particular acquisition activities.[10] Between Acquisition Decision Event 2A and Acquisition Decision Event 2B, the project manager formulates the acquisition into types of acquisition (e.g., capital investment projects, services procurements). The phase concludes with the IRB granting the program approval to proceed at Acquisition Decision Event 3.

[8]According to DHS's *Acquisition Management Directive*, these are acquisition programs whose life cycle cost estimates exceed $300 million or services programs with annual expenditures exceeding $100 million. Major IT acquisitions with life cycle cost estimates between $50 million and $300 million are not reviewed by the IRB.

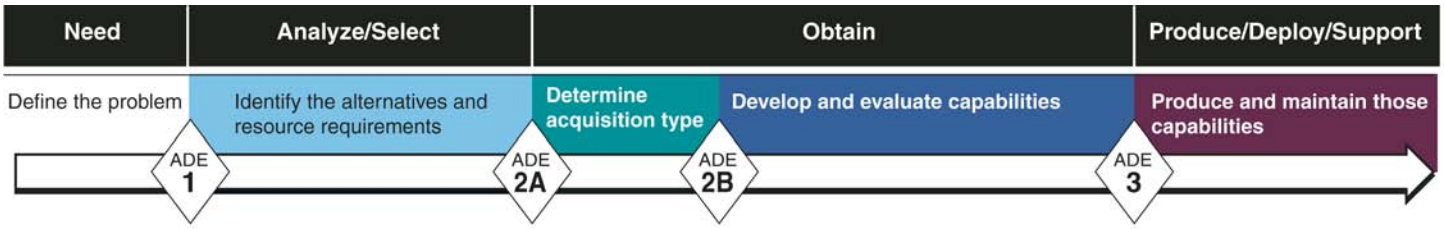
[9]DHS's *Acquisition Directive 102-01* established the Acquisition Review Board as a cross-component group within the department that determines whether a proposed acquisition has met the requirements of key phases in the acquisition life cycle framework and is able to proceed to the next phase and eventual full production and deployment.

[10]During the obtain phase, a program manager may make multiple appearances before the IRB to seek approval for acquisitions needed to support test and evaluation activities for the proposed acquisition. The acquisition decision events are noted as 2B, 2C, etc.

4. The produce/deploy/support phase—during which the process to produce, deploy, and support the needed capability takes place. Although the IRB does not have a standard, defined role in this phase, it may conduct additional reviews as necessary.

Figure 2 presents the four DHS acquisition phases defined in DHS's acquisition directive.

Figure 2: Overview of the DHS Acquisition Phases



Source: GAO analysis of DHS Acquisition Management Directive 102-01.

DHS recently articulated a vision for an Integrated Investment Lifecycle Model as part of a broad effort to improve its overall acquisition management process. The model is intended to help integrate the department's planning, programming, budgeting, and execution processes with the goal of strengthening strategic decision making by implementing a repeatable process at critical phases throughout the investment life cycle. In June 2012, DHS noted that with the early phases of the model's development, a key challenge was developing standardized business terms, data elements, and a central portal to collect, store, and report data. DHS also reported that it planned to complete a concept of operations document and an implementation plan for the Integrated Investment Lifecycle Model concept of operations by the second quarter of fiscal year 2013.

GAO and DHS Have Reported on the Department's Acquisition Management Efforts

Over the years, GAO, the department, and DHS's Office of the Inspector General have reviewed DHS's overall acquisition process, as well as the processes specifically related to its IT acquisitions, identified weaknesses, and provided recommendations for improvements. For example, in April 2007, we reported that although DHS had established the management structure to effectively manage its IT investments, the department had yet

to define most of the policies specifically associated with managing its IT projects as investment portfolios.[11] We also reported that DHS had not fully implemented the key practices needed to actually control investments—either at the project level or at the portfolio level. We recommended that DHS fully define the project-level and portfolio-level policies and procedures defined in GAO's ITIM framework[12] and implement the practices needed to effectively control investments. DHS agreed with our findings and recommendations, and took action to address the majority of them, including augmenting the resources for providing project oversight.

In November 2008, we reported that DHS had not provided the oversight needed to identify and address cost, schedule, and performance problems for its major acquisitions.[13] Specifically, we reported that of the 48 major investments reviewed that required milestone or annual reviews, 45 were not reviewed in accordance with the department's investment review policy, and 18 were not reviewed at all. Four of these investments had transitioned into a late acquisition phase—production and deployment—without any required reviews. We recommended—and DHS concurred—that the department identify and align sufficient management resources to implement oversight reviews in a timely manner throughout the investment life cycle.

In 2010, DHS's Office of the CIO conducted a series of reviews of its major IT programs. According to DHS's draft *Portfolio Governance Concept of Operations*,[14] these reviews, plus additional insights from the CIO, highlighted several problems with the existing IT investment management process, including the following:

[11]GAO, *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, GAO-07-424 (Washington, D.C.: April 27, 2007).

[12]GAO-04-394G.

[13]GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, GAO-09-29 (Washington, D.C.: Nov. 18, 2008).

[14]DHS, *Portfolio Governance Concept of Operations, Draft* (Washington, D.C.: Dec.9, 2011).

- Governance was based on a program-by-program approach that did not reflect the reality that many programs are inter-related in delivering mission outcomes.
- Programs took too long, were often over cost, and did not meet performance objectives.
- Decision makers were often far removed from program details; many decisions were reserved for the IRB, which lacks the capacity and time to be familiar with all mission needs and program issues.

In addition, the department again held portfolio reviews in 2011 and found that while some progress had been made, many of the aforementioned problems continued.

Following the February 2011 update to our high-risk series report on implementing and transforming DHS, in which we reported that while the department had improved its policies and procedures for investment management, more work remained,[15] DHS began providing us with bi-annual updates on its progress in addressing weaknesses, including IT management.[16]

Further, we recently reported that the portfolio reviews DHS conducted in 2011 to avoid investing in systems that were duplicative or overlapping, and to identify and leverage investments across the department contributed to the identification and consolidation of duplicative functionality within four investments.[17] DHS also developed plans to further consolidate systems by 2014, which is expected to produce approximately $41 million in cost savings. The portfolio reviews also contributed to the identification of 38 additional systems that are duplicative.

[15]GAO-11-278.

[16]On June 15, 2012, DHS issued the third bi-annual update on its progress.

[17]GAO, *Information Technology: Departments of Defense and Energy Need to Address Potentially Duplicative Investments*, GAO-12-241 (Washington, D.C.: Feb. 17, 2012).

OMB Has Established Initiatives to Reform Federal IT Investment Management through Portfolio Governance and Accountability

In December 2010, the Office of Management and Budget (OMB) issued its 25 *Point Implementation Plan to Reform Federal Information Technology Management*, a document outlining activities spanning 18 months to reform IT management throughout the federal government. A key goal of the plan—referred to as the IT Reform Plan—is to foster more effective management of large-scale IT programs. One way the plan recommends this be done is through streamlining governance and improving accountability. According to the plan, this involves reforming and strengthening IRBs to enable them to more adequately manage agency portfolios, redefining the role of agency CIOs and the federal CIO Council to focus on portfolio management, and rolling out "TechStat" reviews at the agency and bureau levels to focus attention on IT investments, including those that are poorly performing.[18] In April 2012, we reported that OMB and key federal agencies had made progress on selected action items identified in the IT Reform Plan, but several areas, including strengthening the role of the CIO, were not yet completed.[19]

In an August 2011 memorandum,[20] in conjunction with implementing the IT Reform Plan, OMB clarified the primary areas of responsibility for CIOs throughout the government. It stressed moving the role of CIOs from just policymaking and infrastructure maintenance to encompassing true portfolio management for all IT, which would enable CIOs to focus on delivering solutions that support the mission and business effectiveness of their agencies and overcome bureaucratic impediments to deliver enterprisewide solutions. The memorandum highlighted the role of the CIO to drive the investment review process and to have responsibility over the entire IT portfolio for an agency. In addition, it stated that the CIOs must work with chief financial officers and chief acquisition officers to ensure portfolio analysis is an integral part of the yearly budget process for an agency.

[18]TechStat Accountability Sessions are face-to-face reviews of agency IT programs with OMB and/or agency leadership.

[19]GAO, *Information Technology Reform: Program Made; More Needs to Be Done to Complete Actions and Measure Results*, GAO-12-461 (Washington, D.C.: April 26, 2012).

[20]OMB, *Chief Information Officer Authorities,* M-11-29 (Washington, D.C.: August 8, 2011).

DHS's New IT Governance Process Is Generally Consistent with Best Practices

DHS has defined a vision for its new IT governance process, which includes a three-tiered oversight structure that defines distinct roles and responsibilities from the program through the department. The new governance process is generally consistent with recent OMB guidance and with best practices for managing projects and portfolios, with two practices partially addressed and seven others fully addressed. However, the supporting policies and procedures have yet to be finalized. According to officials, this is because the focus has been on piloting the process. While it is important to conduct pilots to test processes and identify lessons learned, until DHS finalizes its procedures associated with the new IT governance, it will have less assurance that the governance will be consistent with best practices and address previously identified weaknesses in investment management.

DHS's Vision for New IT Governance Process is Based on a Tiered Oversight Structure

In December 2011, the Under Secretary for Management's *Integrated Strategy for High Risk Management* introduced an initiative to improve and streamline IT program execution governance. The initiative established a tiered governance structure for program execution, with specific decision responsibilities for each tier. This structure is intended to supplement, not replace, DHS's existing policies and procedures for managing acquisitions. It also includes several of the governance entities represented in the Integrated Investment Lifecycle Model the department is currently defining to integrate the planning, programming, budgeting, and execution processes.

According to the strategy, the governance process is intended to improve

- IT investment management across DHS by providing enterprise-level governance and oversight based on functional IT portfolios;[21]
- the integration of enterprisewide processes for strategic planning, program management, budget planning, acquisition, and program execution by establishing a tiered governance structure—enterprise, portfolio, and program governance;

[21]Investments are to be vetted to determine the best portfolio based on the functional and technological scope of the investment.

- program health by continuing initiatives to enable IT programs to manage to budget and schedule, mitigate risks, and deliver desired functionality; and

- IT investment performance reporting across the department by leveraging a business intelligence tool—known as the Decision Support Tool—that will provide standardization of data and consistent monitoring of IT portfolios and programs.

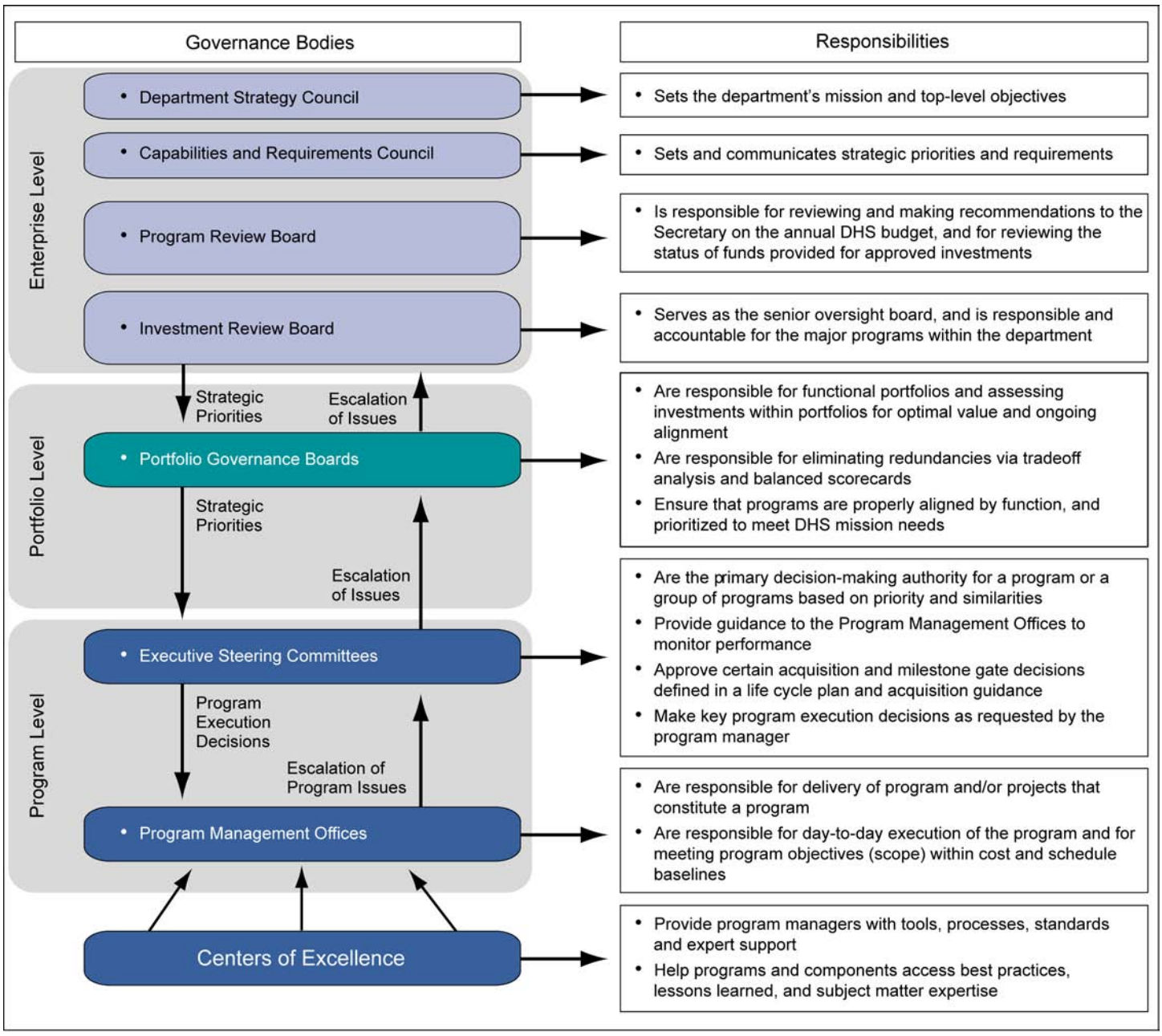
To meet these goals, DHS has defined a scalable, tiered structure among the governance entities that establishes distinct roles and responsibilities from the program through the department. (This structure is illustrated in figure 3.)

- Enterprise level governance—Enterprise governance will focus on setting strategic priorities and requirements to meet the enterprise mission.

- Portfolio level governance—Portfolio governance will manage groups of related programs to ensure that programs are properly aligned and function to meet DHS mission needs.

- Program level governance—Program governance is the primary decision-making authority for individual programs.

Figure 3: DHS's Integrated Enterprise Governance Structure



Source: GAO analysis of DHS data.

Table 1 lists the entities involved in the tiered governance process, and provides a description of their membership. While some of the entities are new, others already existed.

Table 1: IT Governance Entities and Membership

Entity	Membership
Department Strategy Council (New)	Chaired by the Secretary or Deputy Secretary and is to include senior headquarters and component leadership.
Capabilities and Requirements Council (New)	Composed of operational experts from headquarters and components.
Program Review Board	Chaired by the Deputy Secretary and supported by the Office of the Chief Financial Officer's Director for Program Analysis & Evaluation.
IRB	Chaired by the Acquisition Decision Authority, the Under Secretary for Management, and includes the Assistant Secretary for Policy, Under Secretary for Science and Technology, Director of Operational Test and Evaluation, General Counsel, Chief Financial Officer, CIO, Chief Administrative Services Officer, Chief Procurement Officer, Chief Human Capital Officer, Chief Security Officer, other lines of business chiefs as appropriate, user representatives from components sponsoring the capability, and other officials within the department determined to be appropriate to the subject matter by the Acquisition Decision Authority.
Portfolio Governance Boards (New)	The chair for each Portfolio Governance Board is appointed by senior leadership and is supported by members who are senior executives from stakeholder organizations able to contribute relevant expertise and insight to the Portfolio Governance Boards' issues and proceedings.
ESC (New)	Each ESC is chaired by either the DHS CIO or component CIO for critical IT programs. In addition, the Component Acquisition Executive will co-chair ESCs for the component's most critical programs. The board membership will be approved by the IRB and is to include senior executives from program stakeholder organizations who are empowered to make decisions for their organization.
Program Management Offices	Managed by a Program Manager, and supported by a team including a systems engineer, life cycle logistician, Contracting Officer Technical Representative, a business/financial manager and, if applicable, an IT/systems architect.
Centers of Excellence for Program Management (COE)	Headed by a COE lead, and supported by a core leadership team of full-time, dedicated staff. In addition, the membership of a COE will include subject matter experts in specific disciplines from across the department. While these subject matter experts will continue to reside within and report to their home organizations, they will be available for consultation regarding their expertise in a "community of practice" model.

Source: GAO analysis of DHS data.

In addition to the tiered structure intended to improve oversight of programs and portfolios, the IT governance vision also more broadly addresses the process for determining what investments should be selected to address mission gaps (during the planning phase) and ultimately, deliver capabilities (during the execution phase). The following describes these two phases:

- During the *planning phase*, DHS expects to consider IT investments from a departmentwide portfolio perspective, and determine which investments should be funded. To do this, DHS envisions the use of functional portfolios. The portfolios are to align to the 13 functional segments of the department's enterprise architecture and will be governed by the Portfolio Governance Boards.[22] The Department Strategy Council is to provide these portfolios with strategic guidance. Using input from the portfolio managers, the Capabilities and Requirements Council is to adjudicate issues across portfolios and set overall department priorities. In addition, the Portfolio Governance Boards will provide guidance and investment recommendations to the Program Review Board for future year planning, programming, and budgeting. The Program Review Board will then formulate the budget and communicate with OMB and the IRB.

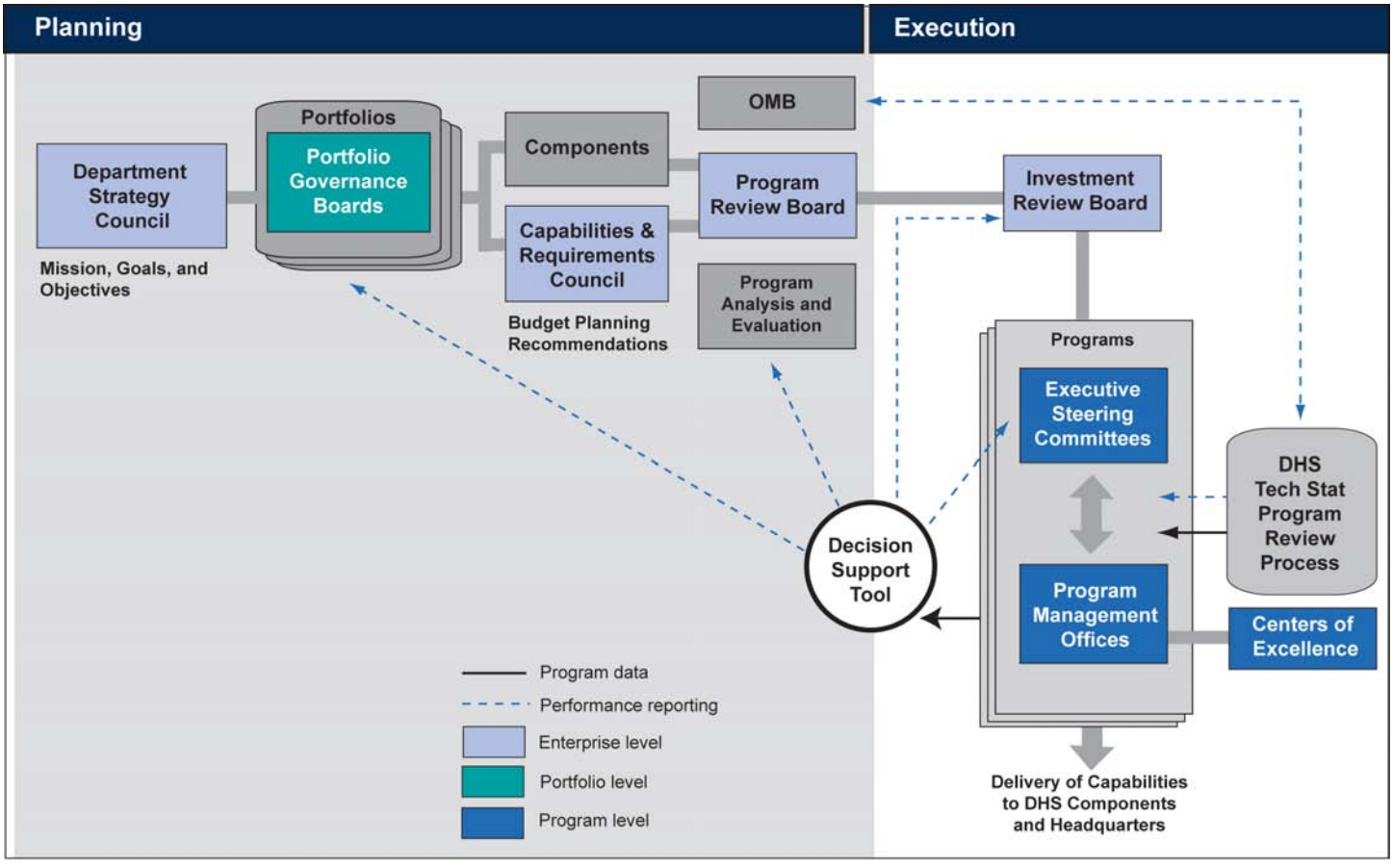
- The *execution phase* is intended to ensure the investments continue to be aligned with the department's strategic goals and fully support mission performance, and ultimately provide the intended capabilities. DHS envisions an interaction among the entities that provide oversight, control, and assistance during program execution—the IRB, the ESCs, and COEs. The ESCs are to oversee major programs or groups of closely related programs. However, if a major program runs into difficultly in its schedule, budget, or scope performance, the program manager would be required to present the status and action plan to the IRB for assessment and approval. This requirement is in addition to the ongoing governance provided by the ESCs. The COEs would provide expert support in core program management disciplines, such as requirements engineering. The department also plans to standardize reviews, including the TechStats and program health assessments. The TechStat reviews are intended to evaluate programs, identify any issues, develop a corrective action plan, and ensure that the program receives proper support to fix the issues. The program health assessments look at individual programs' health in executing and carrying out the program. In fiscal year 2011, DHS performed reviews of 47 IT programs, primarily focusing on those programs with poor performance ratings or deemed highly critical or

[22]The 13 planned portfolios are: Benefits Administration, Continuity of Operations, Domain Awareness, Incident Management, Information Sharing and Safeguarding, Intelligence, Law Enforcement, Screening, Securing, Enterprise Financial Management, Enterprise Human Resource Management, Enterprise IT Services, and Enterprise Business Services.

visible by the CIO. Under the new governance, the Office of the CIO plans to conduct reviews of all 83 major IT investments anywhere from monthly to semi-annually, depending on the health of the project.

According to officials, while the Under Secretary for Management has not yet approved the new IT governance model, DHS has started implementing it. Figure 4 shows the recommended process for determining what investments should go forward, providing oversight, and delivering capabilities.

Figure 4: DHS's Recommended IT Governance Operating Model



Source: GAO analysis of DHS data.

In addition, DHS plans to use its Decision Support Tool to provide updated program information to all governance bodies on the status of major programs. The Decision Support Tool is to provide the ability to

integrate data resident within multiple existing source systems including the Next Generation Periodic Reporting System and the Investment Management System, to generate reports, charts and graphs on program performance.[23]

DHS's New IT Governance Framework Is Generally Consistent with Guidance, Best Practices, but Policies and Procedures Have Not Yet Been Finalized

DHS's new IT governance framework is generally consistent with recent OMB guidance. Specifically, consistent with OMB guidance calling for the CIO to play a significant role in the oversight of the portfolio of IT programs, DHS's draft procedures note that ESCs overseeing IT programs must include the DHS CIO, a component CIO, or a designated executive representative from a CIO office. In addition, for programs that the DHS CIO Council designates as most critical, the DHS CIO or an appropriate component CIO will co-chair the ESC. Further, consistent with recent OMB guidance to focus on portfolio management, the new governance framework includes the establishment of portfolio governance boards to oversee functional portfolios with the goals of eliminating duplication and leveraging services and programs across the department.

In addition, DHS's new IT governance framework and the associated policies and procedures are generally consistent with best practices for managing projects and portfolios identified in GAO's ITIM framework, with two practices partially addressed and seven others fully addressed; however, the procedures have not been finalized. Tables 2 and 3 summarize our assessment of DHS's draft procedures against relevant practices of our ITIM.

[23]The Next Generation Periodic Reporting System captures contract, project and program level data for quarterly and monthly reporting. It supports portfolio reviews at the DHS, component, program, and project levels and enables users to conduct analysis, trending, and forecasting at these levels and allows users to generate reports. The Investment Management System supports DHS's capital planning process and is used, among other things, to capture and report on business case information, such as in Exhibit 300 submissions.

Table 2: Assessment of Policies and Procedures for Program Management

Practice category	Specific practice	Assessment	Summary of evidence
Instituting Investment Board Operations	In cases where lower-level investment boards (such as the ESCs) are chartered to carry out the responsibilities of the enterprisewide IT investment board within their own business units, the enterprisewide IT investment board still must maintain ultimate responsibility for—and therefore visibility into—the lower-level boards' activities.	Partially addressed	According to the draft program governance procedures, if a program that has been assigned to an ESC experiences schedule, budget, or scope problems, the program manager must present a status and action plan to the IRB for assessment and approval. In addition, the IRB is to reassume acquisition decision authority if a program is in breach of cost, schedule or performance goals established in the acquisition program baseline until the program has taken corrective actions, rebaselined the program with an IRB-approved acquisition program baseline, and the IRB authorizes the ESC to reassume acquisition decision authority. These requirements, however, are not established in policies and procedures such as the Program Governance Concept of Operations document, which would have broader applicability. Further, while in practice, the department maintains visibility into the ESC activities by having the CIO—who is a member of the IRB—chair or attend meetings, the policies and procedures supporting the new IT governance process do not address this or reference existing documents which might address this.
	The enterprisewide IT investment board should be responsible for major systems that affect multiple components and users, and stay actively involved in those that are high cost or high risk or have significant scope and duration.	Fully addressed	As previously stated, the board maintains responsibility for major IT investments with life cycle cost estimates of $300 million or more. While ESCs may oversee these investments, they are only expected to receive authority to approve certain acquisition decision events. In addition, as stated above, depending on the status of a program, this decision authority could be rescinded. Further, according to the draft program governance procedures, if a program experiences schedule, budget, or scope problems, the program manager must present a status and action plan to the IRB for assessment and approval.
	Investment management guidance should specify the manner in which IT investment-related processes will be coordinated with other organizational plans, processes, and documents—including, at a minimum, the strategic plan, budget, and enterprise architecture processes.	Fully addressed	DHS's draft portfolio governance procedures indicate that portfolio activities include executing suitability analysis, adding and ranking investments into the rolling 5-year strategy and enterprise architecture transition plan, requesting budget approval, and tracking continuing status and performance of programs underway.

Practice category	Specific practice	Assessment	Summary of evidence
	Subordinate boards should have the same broad business unit and IT representation as the enterprisewide board.	Fully addressed	DHS's draft governance procedures specify that the composition of the ESCs and Portfolio Governance Boards should include both business and technical representation.
Selecting an Investment	Policies and procedures for effectively selecting investments for funding typically outline a structured method for identifying, evaluating, prioritizing, and selecting new IT investment proposals, including criteria to support the analysis, prioritization, and selection of new investments. Similar policies and procedures should exist for reselecting ongoing investments	Partially addressed	DHS's draft portfolio governance policies and procedures address the selection of proposed investments and the reselection of existing investments. They specify a process for the review and selection of proposed investments, requiring a Portfolio Governance Board to rank a proposed investment's relative priority with all other approved investments in order to formally add it to the portfolio transition plan. This plan is to represent a point of reference to which DHS investments, both legacy and new investments approved for execution, are identified. The draft procedures also specify that the review of an investment must use existing DHS selection and prioritization criteria, such as resources needed and benefits to be derived. However, the draft procedures do not specify these criteria or reference other documents where these criteria may be identified.
Providing Investment Oversight	Procedures for providing investment oversight typically specify the procedural rules for investment boards' operation and for decision making during program oversight; the criteria that the investment boards use when analyzing project performance as part of their oversight function; that corrective actions are required when the project deviates or varies significantly from the project management plan; and the procedures for escalating unresolved or significant issues.	Fully addressed	As stated above, the board maintains responsibility for major IT investments.

Practice category	Specific practice	Assessment	Summary of evidence
Capturing Investment Information	Procedures for capturing investment information typically specify that responsibility for submitting, updating, and maintaining relevant inventory information for each project or asset is explicitly assigned; the process to be followed for the collection of information, access to the information, and support for maintaining the information; the data elements required for each IT-related item, including the cost (e.g., history of actual development costs, annual operating and maintenance costs, and expected life cycle costs) of each item; and the owner of each item.	Fully addressed	In February 2012, the Under Secretary for Management directed the implementation of the enterprise Decision Support Tool to improve the department's governance capabilities, as well as aid departmental strategic acquisition decision making. The tool is to integrate and enhance the functionalities of existing systems used throughout DHS in order to generate integrated, high-quality data on program performance. It is to establish standard content, format, and frequency for investment performance analysis and reporting, including key risks and mitigation plans. In addition, the tool is to allow the stakeholders to efficiently report program health status to the Portfolio Governance Board using a format that is consistent across portfolios, programs, and governance bodies. PARM officials stated that component acquisition executives are to be responsible for the completeness of the data in the tool, and accuracy for their respective programs. DHS is deploying the Decision Support Tool in phases as it addresses additional requirements.

Source: GAO analysis of DHS data.

Table 3: Assessment of Policies and Procedures for Portfolio Management

Practice category	Specific practices	Assessment	Summary of evidence
Creating the Portfolio	The organization's policies and procedures for analyzing and developing IT investment portfolios typically provide common definitions for IT investment portfolio categories, apply to each IT investment board as it develops its comprehensive portfolio, and stipulate conditions that should be met for investment funding decisions where exceptions are made.	Fully addressed	DHS's draft portfolio governance procedures identify the steps that will be taken to approve proposed investments and assign them to the appropriate functional portfolio. In addition, the procedures state that after investment proposals are analyzed by the enterprise architecture organization to assess potential overlap or duplication, they must then go through a suitability analysis to determine the functional and technological scope of the investment proposals. After the investment has been approved, the procedures further call for an analysis of the investment's alignment with the DHS strategic goals, which will assist in ranking the new investment's priority relative to the others in that portfolio.
Evaluating the Portfolio	The organization should have documented policies and procedures for reviewing, evaluating, and improving the performance of its portfolios. This includes defining and collecting performance data that is consistent with established portfolio performance criteria, and making adjustments to the IT investment portfolio in response to actual performance.	Fully addressed	In DHS's draft portfolio governance procedures, the department identified specific portfolio governance critical success factors—such as having proactive executives and subject matter experts—to ensure its investments are defined and planned in the most effective way in order to lead to a greater probability of success. The document also identified key performance indicators, such as progress in meeting strategic objectives and timely decision making to gauge portfolio performance.

Source: GAO analysis of DHS data.

According to officials, the policies and procedures supporting DHS's new IT governance have not been finalized because the focus has been on piloting the new governance process. To the department's credit, according to officials, the Portfolio Governance Concept of Operations, which focuses more on the role of the Portfolio Governance Boards, is expected to be approved by the end of July. In addition, the Program Governance Concept of Operations, which is intended to specify how programs are to be overseen, is currently being drafted and expected to be finalized in August 2012 (and approved by the CIO later). Further, according to officials, resources have recently been assigned to updating DHS's current *Information Technology Integration and Management* directive to reflect the new framework, and work has also begun to update the *Acquisition Management Directive*. While the use of pilots is valuable in testing processes and identifying lessons learned, until DHS finalizes the policies and procedures associated with the new IT governance, the department will have less assurance that its new IT governance will be

consistent with best practices and address previously identified weaknesses in investment management.

DHS Has Implemented Aspects of Its New Structure, but Has Not Fully Followed Best Practices

DHS has begun to implement components of the IT governance framework. Specifically, the department has primarily focused its implementation efforts on the "execution" phase of the IT governance operating model (see fig. 4) because, according to officials, it includes the department's more mature processes. Efforts to implement other aspects of the model have been more limited.

Table 4 below shows the status of the implementation of the governance bodies.

Table 4: Status of the Implementation of Governance Entities

Governance entity	Status
IRB	This board pre-dates the new governance structure. It has been operating and holding meetings.
Capabilities and Requirements Council	According to officials, this group is not yet established.
Department Strategy Council	According to officials, this council is not yet established.
Portfolio Governance Boards	Currently three Portfolio Governance Boards are operational, and two are expected to become operational by the end of this fiscal year. DHS's three current portfolio governance boards are the Information Technology Services Governance Board, Information Sharing & Safeguarding Governance Board, and Human Resources Information Technology. The two planned for completion by the end of the fiscal year are Screening and Integrated Domain Awareness. According to the CIO, the vision is to have one Portfolio Governance Board for each of DHS's 13 functional portfolios.
Program ESCs	DHS has initiated pilot ESCs to test aspects of the new governance structure. Specifically, the CIO identified an initial set of 16 high-visibility programs to be overseen by ESCs[a] According to the CIO, DHS envisions assigning larger, more complex, higher visibility or riskier programs to an ESC.
COE	DHS has established seven COEs to support program management, and, according to officials, recently established an eighth one[b] In addition, a COE Council and COE Coordinating Office have been established. Officials stated that they are still in the process of conducting a resource assessment for developing a Federated Governance Staffing Requirements Plan. This should contribute to identifying staff with needed expertise to serve as subject matter experts for the COEs.

Source: GAO analysis of DHS data.

[a]The 16 high-visibility programs are: Automated Commercial Environment/International Trade Data Systems; Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance; Customs and Border Protection's Traveler Enforcement Compliance System Modernization; Homeland Security Network; Homeland Security Presidential Directive 12 Identity, Credential, and Access Management; Immigration and Customs Enforcement's Traveler Enforcement Compliance System Modernization; Infrastructure Transformation Program; National Cyber Security Protection System; National Flood Insurance Program; Next Generation Tactical Communications; Student and Exchange Visitor Information System II; Technical Infrastructure Modernization; United States Citizenship and Immigration Services Transformation; United States Visitor & Immigrant Status Indicator Technology; United States Secret Service Information Integration and Transformation; and Verification Information System/Employment Eligibility Verification.

[b]The seven COEs are: Program Management, Test and Evaluation, Enterprise Architecture, Accessibility, Requirements Engineering, Cost Estimating, and Privacy. According to officials, a Systems Engineering COE was recently established.

In addition to progress made with the governance entities above, DHS has also taken other steps to implement the new IT governance structure.

- *Portfolio reviews:* According to the CIO, the department is currently performing portfolio reviews in collaboration with PARM and the Office of the Chief Financial Officer. These reviews look at the alignment of a functional grouping of investments and the mission effectiveness, or value, those investments deliver. The focus of these reviews is to identify overlaps and redundancies in existing investments, and to

identify gaps in existing capabilities. According to the Deputy CIO, these portfolio reviews represent a new way of operating for the components, as they were not used to looking at functions across the department, only portfolios within their respective components. According to the CIO, as the Portfolio Governance Boards are established, they are expected to take over the role of reviewing these portfolios.

- *Program reviews:* In fiscal year 2011, the CIO's office performed program health assessment reviews of 47 IT programs, primarily focusing on those programs with poor performance ratings or determined to be highly critical or visible by the CIO. According to officials, all 83 major IT investments have been reviewed for this fiscal year.

- *TechStat reviews:* According to officials, the Office of the CIO also performed two TechStat reviews in fiscal year 2011, and three of the four TechStats planned for fiscal year 2012. In addition, officials stated they have completed TechStat training for 12 components.

DHS Is Taking Steps to Obtain Organizational Buy-in

According to industry best practices, in order to effectively implement a new IT governance framework, or any large organizational change, organizations should obtain buy-in by involving all key stakeholders to ensure key perspectives are considered and facilitate adoption. This includes having top management support and creating forums for involving business representatives.

DHS has top management support, as evidenced by the Under Secretary for Management approving key documents supporting the new governance process. For example, the December 2011 *Integrated Strategy for High Risk Management*, which introduces the vision for the IT governance structure, was approved by the Under Secretary for Management. The Under Secretary also issued a memorandum calling for the use of pilot ESCs and providing these ESCs authority to oversee investment performance. In addition, to secure buy-in, EBMO also sought comments on a draft of its *Portfolio Governance Concept of Operations*, and, according to officials communicated its efforts to improve IT investment management to senior executives (including the Chief Financial Officer and Chief Procurement Officer) and to the components. According to the EBMO Director, these stakeholders' participation on ESCs or portfolio review boards and involvement in conducting the portfolio reviews has also helped to secure their buy-in. Taking these steps increases the likelihood that the new IT governance process will be

adopted despite the significant cultural change it represents. The CIO and Executive Director for EBMO both noted that the new governance is gradually gaining acceptance.

An Implementation Team Has Been Established, but the Department Lacks an Implementation Plan

Effectively implementing a new IT governance process also requires developing an effective implementation team and plan. According to best practices, an effective implementation team should be put in place that includes key stakeholders from both business and IT components. In addition, we have previously reported that to effectively implement IT investment management processes, organizations need to be guided by a plan that builds on existing strengths and weaknesses; specifies measurable goals, objectives, and milestones; specifies needed resources; assigns clear responsibility and accountability for accomplishing tasks; and is approved by senior-level management.[24] Such a plan is instrumental in helping agencies coordinate and guide improvement efforts.

DHS has established an integrated product team to guide the implementation of the new IT governance structure. According to DHS officials, the department's integrated product team is made up of officials from EBMO, PARM, and the department's chief executives (e.g., CIO, Chief Financial Officer, etc.). Further, according to the department, the EBMO senior staff directly involved with the implementation of the governance structure have both program-level and portfolio-level governance experience. According to officials, the integrated product team is supported by subject matter experts and the Component Acquisition Executives.

However, the department has not yet developed an implementation plan. While DHS's June 2012 *Integrated Strategy for High Risk Management* includes components of an implementation plan, such as high-level goals and activities to be completed by the end of fiscal year 2012, DHS does not have an implementation plan addressing the elements mentioned above. While officials recognized the value of an implementation plan, they stated they had not yet developed one because they are still piloting the new governance process. Further, officials stated that they planned

[24]GAO, *Information Technology: Treasury Needs to Strengthen Its Investment Board Operations and Oversight*, GAO-07-865 (Washington, D.C.: July 23, 2007).

on developing a 2-year implementation plan that would incorporate best practices identified in the ITIM framework for effectively managing projects and portfolios. They stated that this plan would draw from the department's revised IT strategic plan due to be completed by the end of the summer of 2012. To mitigate for the limited resources available, DHS states it will adopt a federated model for resources—drawing resources from components—and use contractor support, as needed. Until a plan is developed, the department may not be able to effectively implement the new IT governance process to ensure that it addresses previously identified weaknesses, and effectively uses the department's limited resources.

DHS Has Yet to Fully Define Processes for Evaluating Its Implementation Efforts

According to best practices, when implementing an IT governance framework, it is important to evaluate the implementation efforts by, among other things, developing measures to assess progress in meeting objectives. In addition, according to best practices, when implementing a new governance framework, there should be mechanisms in place to document lessons learned for subsequent governance improvement initiatives. According to our ITIM framework, among other things, lessons learned and recommendations for improving the investment process should be developed and documented, and then distributed to all stakeholders.

DHS has defined measures in the June 2012 update to the *Integrated Strategy for High Risk Management*. For example, DHS plans to measure the (1) percentage of DHS IT program reviews completed in fiscal year 2012; (2) percentage of DHS IT programs rated as low risk; (3) percentage of IT investment portfolio governance boards and ESCs established and chartered; and (4) percentage of components trained and conducting component-led TechStats. In addition, the department has identified measures to assess the effectiveness of the ESC program reviews. Further, according to officials, draft measures for the COE functions have also been developed; however, they have not yet been documented and officials did not have any time frames for doing so. Without fully defining and documenting measures of success, it is unlikely that the department will be able to determine if it has successfully and efficiently established its new IT governance framework.

DHS officials stated that they are using lessons learned from their piloting activities to improve their governance process; however, they have not established a mechanism for capturing lessons learned. Without this mechanism, the department risks not being able to continue to build on

the experiences and lessons learned from prior initiatives, which could help to identify, introduce, and sustain additional efficiency gains on a more systematic basis.

Conclusions

DHS's new approach to IT governance shows promise in establishing mechanisms for greater oversight, involving key staff in program decisions, and focusing on functional portfolios in order to avoid unnecessary duplication. To the department's credit, the vision is generally consistent with guidance and with best practices for managing projects and portfolios. However, we identified two practices which were only partially addressed in policies and procedures—ensuring that the IRB maintains visibility into the activities of the ESCs, and defining project selection and prioritization criteria—which could limit the extent to which these practices are institutionalized. In addition, the policies and procedures have not yet been finalized. To its credit, DHS has efforts underway to address this. However, until DHS finalizes these policies and procedures and ensures that they fully address practices for managing programs and portfolios of investments, the department will have less assurance that its new approach will address identified weaknesses and facilitate effective governance.

DHS has implemented aspects of its new approach, such as establishing governance entities associated with the execution phase of its approach and conducting portfolio and program reviews. However, because the agency has not developed an implementation plan, fully documented performance measures, or established a mechanism for capturing lessons learned, there is a risk that the approach may be less effective than intended.

Recommendations for Executive Action

To implement an effective IT governance strategy, we recommend that the Secretary of Homeland Security direct the appropriate officials to finish defining the new IT governance process by

- finalizing the IT governance policies and procedures and ensuring they fully address or reference existing documents that address the following:
    - how the IRB is to maintain responsibility for lower-level board activities; and

- investment selection and prioritization criteria.

In addition, to assist in implementing the new IT governance strategy, we recommend that the Secretary of Homeland Security direct the appropriate officials to

- develop an implementation plan that draws together ongoing and additional efforts needed to implement the new IT governance process. The plan should:

  1. build on existing strengths and weaknesses;
  2. specify measurable goals, objectives, and milestones;
  3. specify needed resources;
  4. assign clear responsibility and accountability for accomplishing tasks; and
  5. be approved by senior-level management.

- fully define and document key measures to monitor the implementation process; and
- establish mechanisms for capturing lessons learned.

Agency Comments and Our Evaluation

DHS's Director for the Departmental GAO-OIG Liaison Office provided written comments on a draft of this report (reprinted in appendix II). He stated that the department was pleased to note GAO's positive acknowledgement that DHS's IT governance framework was consistent with OMB guidance and GAO's ITIM framework. He also stated that the department concurred with the recommendations and estimated it would address them by September 30, 2013. The department also provided technical comments, which we have incorporated where appropriate.

We are sending copies of this report to interested congressional committees and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staffs have any questions on the matters discussed in this report, please contact me 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. GAO staff who made major contributions to this report are listed in appendix III.

David A. Powner
Director, Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) describe the Department of Homeland Security's (DHS) new information technology (IT) governance process and associated policies and procedures, and assess them against best practices; and (2) determine progress made in implementing the new approach and how DHS's implementation efforts comport with relevant best practices.

To address our first objective, we reviewed and analyzed documentation on DHS's newly initiated IT governance process. This documentation included the Under Secretary for Management's *Program Management & Execution Playbook*, the December 2011 biannual update to the Implementation and Transformation section of DHS's Integrated Strategy for High Risk Management, the Office of the Chief Information Officer's Concept of Operations documents for Program and Portfolio Governance, and Chief Information Officer quarterly update briefings presented to GAO. We also reviewed various memorandums from the Under Secretary for Management, which covered such issues as the chartering of Executive Steering Committees and the implementation of the department's Decision Support Tool. We also interviewed officials from DHS's Office of the Chief Information Officer's Enterprise Business Management Office (EBMO), and from the Office of Program Accountability and Risk Management (PARM). To assess DHS's vision of its planned governance process against GAO's Information Technology Investment Management (ITIM) guide,[1] we identified the ITIM stage 2 and stage 3 critical process areas that were most relevant to DHS's efforts, and compared the evidence collected from our document reviews and interviews to the practices associated with these areas.

To address our second objective, we obtained and evaluated documentation showing the department's efforts in implementing the governance process. This included documentation defining the roles of various governance entities, such as the Executive Steering Committees and Portfolio Governance Boards, to be involved in the process. We reviewed available charters and meeting minutes for several of these entities to determine if they were functioning. We also reviewed documentation on the Centers of Excellence established by DHS to provide subject matter expertise to support program management. In

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

addition, we interviewed officials from EBMO and PARM to determine the status of the department's effort's in implementing the governance process. We also requested information from the five programs for which Executive Steering Committees were first established on the various reviews they had undergone since January 2010—including type of review, time frames for each review, and information requested—to determine the extent of duplication or overlap among the reviews. In order to assess DHS's implementation of the IT governance approach against accepted best practices, we first used content-analysis software to identify best practices shared by industry and the federal government. We identified these practices from prior our reports, Office of Management and Budget guidance, and guidance from recognized experts in IT governance.[2] We grouped the practices into three categories—(1) organizational buy-in, (2) development of an implementation team and implementation plan, and (3) evaluation— and determined from the evidence collected from our document reviews and interviews the extent to which DHS was following these best practices.

We conducted this performance audit from October 2011 to July 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[2]These include, among others, IT Governance Institute, Gartner, IBM, and Oracle.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

July 17, 2012

David A. Powner
Director, Information Technology Management Issues
441 G Street, NW
U.S. Government Accountability Office
Washington, DC 20548

Re: Draft Report GAO-12-818, "INFORMATION TECHNOLOGY: DHS Needs to Further Define and Implement Its New Governance Process"

Dear Mr. Powner:

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 and Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgement that DHS's Information Technology (IT) governance framework is consistent with recent Office of Management and Budget guidance and best practices for managing projects and portfolios identified in GAO's IT Investment Management (ITIM) Framework. DHS has made significant progress in achieving ITIM compliance as represented by addressing all practice categories for Program Management, including instituting investment board operations and providing investment oversight. In addition, the Department has completely addressed the two practice categories for Portfolio Management.

The draft report contained two recommendations with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct the appropriate officials to finish defining the new IT governance process by finalizing the IT governance policies and procedures and ensuring they address or reference existing documents that address the following:

- how the IRB is to maintain responsibility for lower-level board activities; and
- investment selection and prioritization criteria.

Response: Concur. The Enterprise Business Management Office (EBMO) within OCIO (Office of the Chief Information Officer) will finalize policies and procedures that support IT governance and ensure they address or reference the Investment Review Board (IRB) retention of responsibility for lower level board activities and investment selection and prioritization criteria. Estimated Completion Date (ECD): September 30, 2013

Recommendation 2: Assist in implementing the new IT governance strategy. Specifically:

- develop a coordinated implementation plan that draws together ongoing and additional efforts needed to implement the new IT governance process. The plan should:
  1) build on existing strengths and weaknesses
  2) specify measurable goals, objectives, and milestones
  3) specify needed resources
  4) assign clear responsibility and accountability for accomplishing tasks, and
  5) be approved by senior-level management.
- Fully define and document key measures to monitor the implementation process; and,
- Establish mechanisms for capturing lessons learned.

Response: Concur. The DHS OCIO EBMO will work within the Governance Integrated Project Team to develop an implementation plan. The implementation plan will build upon existing strengths, include measurable goals, objectives and milestones, identify resources with clear responsibility for accomplishing tasks, define and document measures to monitor implementation, identify methods for capturing lessons learned and be approved by senior management. ECD: September 30, 2013

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, the following staff also made key contributions to this report: Sabine R. Paul, Assistant Director; William G. Barrick; Sairah R. Ijaz; Lee A. McCracken; and Tomas Ramirez.