United States Government Accountability Office

GAO

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 7, 2011

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

Statement of Gene L. Dodaro
Comptroller General of the United States

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-919T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.

September 7, 2011

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

Why GAO Did This Study

The terrorist attacks of September 11, 2001, led to profound changes in government agendas, policies and structures to confront homeland security threats facing the nation. Most notably, the Department of Homeland Security (DHS) began operations in 2003 with key missions that included preventing terrorist attacks from occurring in the United States, reducing the country's vulnerability to terrorism, and minimizing the damages from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. Since 2003, GAO has issued over 1,000 products on DHS's operations in such areas as border and transportation security and emergency management, among others. As requested, this testimony addresses DHS's progress and challenges in implementing its homeland security missions since it began operations, and issues affecting implementation efforts. This testimony is based on a report GAO is issuing today, which assesses DHS's progress in implementing its homeland security functions and work remaining.

What GAO Recommends

While this testimony contains no new recommendations, GAO previously made about 1,500 recommendations to DHS. The department has addressed about half of them, has efforts underway to address others, and has taken additional action to strengthen its operations. In commenting on GAO's report upon which this testimony is based, DHS stated that the report did not address all of DHS's activities. The report was based on prior work, which GAO reflected throughout the report.

View GAO-11-919T or key components. For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

Since it began operations in 2003, DHS has implemented key homeland security operations and achieved important goals and milestones in many areas to create and strengthen a foundation to reach its potential. As it continues to mature, however, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. DHS's accomplishments include developing strategic and operational plans; deploying workforces; and establishing new, or expanding existing, offices and programs. For example, DHS

- issued plans to guide its efforts, such as the Quadrennial Homeland Security Review, which provides a framework for homeland security, and the National Response Framework, which outlines disaster response guiding principles;
- successfully hired, trained, and deployed workforces, such as a federal screening workforce to assume security screening responsibilities at airports nationwide; and
- created new programs and offices to implement its homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to help coordinate efforts to address cybersecurity threats.

Such accomplishments are noteworthy given that DHS has had to work to transform itself into a fully functioning department while implementing its missions—a difficult undertaking that can take years to achieve. While DHS has made progress, its transformation remains high risk due to its management challenges. Examples of progress made and work remaining include:

Border security. DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology program to verify the identities of foreign visitors entering and exiting the country by processing biometric and biographic information. However, DHS has not yet determined how to implement a biometric exit capability and has taken action to address a small portion of the estimated overstay population in the United States (individuals who legally entered the country but then overstayed their authorized periods of admission). DHS also deployed infrastructure to secure the border between ports of entry, including more than 600 miles of fencing. However, DHS experienced schedule delays and performance problems with the Secure Border Initiative Network, which led to the cancellation of this information technology program.

Aviation security. DHS developed and implemented Secure Flight, a program for screening airline passengers against terrorist watchlist records. DHS also developed new programs and technologies to screen passengers, checked baggage, and air cargo. However, DHS does not yet have a plan for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements, a mechanism to verify the accuracy of data to help ensure that air cargo screening is being conducted at reported levels, or approved technology to screen cargo once it is loaded onto a pallet or container.

Emergency preparedness and response. DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-

based preparedness, and a Target Capabilities List to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS is also finalizing a National Disaster Recovery Framework. However, DHS needs to strengthen its efforts to assess capabilities for all-hazards preparedness, and develop a long-term recovery structure to better align timing and involvement with state and local governments' capacity. DHS should also improve the efficacy of the grant application process by mitigating duplication or redundancy within the various preparedness grant programs.

Chemical, biological, radiological and nuclear (CBRN) threats. DHS assessed risks posed by CBRN threats and deployed capabilities to detect CBRN threats. However, DHS should work to improve its coordination of CBRN risk assessments, and identify monitoring mechanisms for determining progress made in implementing the global nuclear detection strategy.

GAO's work identified three themes at the foundation of DHS's challenges.

Leading and coordinating the homeland security enterprise. DHS has made important strides in providing leadership and coordinating efforts among its stakeholders. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In 2005, GAO designated information sharing for homeland security as high risk because the federal government faced challenges in analyzing and sharing information in a timely, accurate, and useful way.

Implementing and integrating management functions for results. DHS has enhanced its management functions, and has plans in place to further strengthen the management of the department for results. However, DHS has not always effectively executed or integrated these functions. In 2003, GAO designated the transformation of DHS as high risk because DHS had to transform 22 agencies into one department. DHS has demonstrated strong leadership commitment and begun to implement a strategy to address its management challenges. However, these challenges have contributed to schedule delays, cost increases, and performance problems in major programs aimed at delivering important mission capabilities, such as the Coast Guard's Deepwater Program to modernize ships and aircraft. DHS also faced difficulties in deploying technologies that meet defined requirements. Further, DHS does not yet have enough skilled personnel to carry out activities in various areas, such as acquisition management; and has not yet developed an integrated financial management system, impacting its ability to have ready access to reliable information for informed decision making.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats have impacted DHS's approaches and investments. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs in an efficient manner.

Given DHS's leadership responsibilities in homeland security, it is critical that its programs are operating as efficiently and effectively as possible, are sustainable, and continue to mature to address pressing security needs. Eight years after its creation and 10 years after September 11, 2001, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee:

I am pleased to be here today to discuss our work on progress made by the Department of Homeland Security (DHS) and work remaining in implementing its homeland security missions since it began operations in March 2003. The nation is about to pass the 10-year anniversary of the September 11, 2001, terrorist attacks. The events of that day led to profound changes in government agendas, policies, and structures to confront homeland security threats facing the nation. This milestone provides an opportunity to reflect on the progress DHS has made since its establishment and challenges it has faced in implementing its missions, as well as to identify issues that will be important for the department to address as it moves forward, based on work we have completed on DHS programs and operations in key areas.

DHS was established with key missions that include preventing terrorist attacks from occurring within the United States, reducing U.S. vulnerability to terrorism, minimizing resulting damages, and helping the nation recover from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. We have evaluated numerous departmental programs since DHS began its operations, and issued more than 1,000 reports and congressional testimonies in areas such as border security and immigration, transportation security, and emergency management, among others.

We have made approximately 1,500 recommendations to DHS designed to strengthen its operations, such as to improve performance measurement efforts, strengthen management processes, enhance coordination and information sharing, and increase the use of risk information in planning and resource allocation decisions, as well as to address gaps and challenges in its mission operations that have affected DHS's implementation efforts. DHS has implemented about half of these recommendations, has actions underway to address others, and has taken additional steps to strengthen its mission activities.

However, we reported that the department has more to do to ensure that it conducts its missions efficiently and effectively, while simultaneously preparing to address future challenges that face the department and the nation. Addressing these issues will likely become increasingly complex as domestic and world events unfold, and will be particularly challenging in light of the current fiscal environment and constrained budgets.

In 2003, we designated the implementation and transformation of DHS as high risk because it represented an enormous undertaking that would require time to achieve in an effective and efficient manner.[1] Additionally, the components that merged to form DHS already faced a wide array of existing challenges, and any DHS failure to effectively carry out its mission could expose the nation to potentially serious consequences. The area has remained on our high-risk list since 2003.[2] Our prior work on mergers and organizational transformations, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take years to achieve.[3]

In 2007, we reported on progress made by DHS in implementing its mission and management functions by assessing actions DHS took to achieve performance expectations within each function.[4] We reported that DHS made progress in implementing all of its mission and management functions since it began operations, but progress among the areas varied significantly. For example, we reported that DHS made more progress in implementing its mission functions than its management functions. We also reported that DHS generally had not established

[1] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003). In addition to this high-risk area, DHS has responsibility for other areas we have designated as high risk. Specifically, in 2005 we designated information sharing for homeland security as high risk, involving a number of federal departments including DHS, and in 2006, we identified the National Flood Insurance Program as high risk. Further, in 2003 we expanded the scope of the high-risk area involving federal information security, which was initially designated as high-risk in 1997, to include the protection of the nation's computer-reliant critical infrastructure.

[2] GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

[3] See GAO, *Highlights of a GAO Forum: Mergers and Transformations: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, GAO-03-293SP (Washington, D.C.: Nov. 14, 2002), and *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

[4] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007). We defined performance expectations as a composite of the responsibilities or functions—derived from legislation, homeland security presidential directives and executive orders, DHS planning documents, and other sources—that the department was to achieve or satisfy in implementing efforts in its mission and management areas. The performance expectations were not intended to represent performance goals or measures for the department.

quantitative goals and measures for assessing its performance and, as a result, we could not assess where along a spectrum of progress DHS stood in achieving its missions. Subsequent to the issuance of this report, DHS continued to take action to strengthen its operations and the management of the department, including enhancing its performance measurement efforts. At the request of this Committee, following the issuance of our report, we provided DHS with feedback on the department's performance goals and measures as DHS worked to better position itself to assess its results. Based on its internal review efforts and our feedback, DHS took action to develop and revise its performance goals and measures in an effort to strengthen its ability to assess its outcomes and progress in key mission areas. For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its Quadrennial Homeland Security Review (QHSR) missions and goals.[5] The department plans to report on its results in meeting established targets for these new measures at the end of the fiscal year.

In February 2010, DHS issued its first QHSR report, outlining a strategic framework for homeland security to guide the activities of the department and its homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations. The report identified five homeland security missions—Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Securing Cyberspace, and Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission. In addition, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR), a departmentwide assessment to align DHS's programmatic activities, such as investigating drug smuggling and

[5] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010). The Implementing Recommendations of the 9/11 Commission Act required that beginning in 2009, and every 4 years thereafter, DHS conduct a quadrennial review that provides a comprehensive examination of the homeland security strategy of the United States. Pub. L. No. 110-53, § 2401(a), 121 Stat. 266, 543-45 (2007) (codified at 6 U.S.C. § 347).

inspecting cargo at ports of entry, and its organizational structure to the missions and goals identified in the QHSR.[6]

My statement is based on a report we are issuing today assessing DHS's programs and operations.[7] As requested, the report and my statement address the progress made by DHS in implementing its homeland security missions since it began operations, remaining work, and crosscutting and management issues that have affected DHS's implementation efforts.

The report is based on our work on DHS since it began operations, supplemented with work completed by the DHS Office of Inspector General (IG), with an emphasis on work completed since 2008 to reflect recent work, and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on some DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, as well as updated information provided by DHS, we examined program documentation and interviewed agency officials, among other things. This statement highlights key, recent work at DHS, but does not address all products we and DHS IG issued related to the department, nor does it address all of DHS's homeland security-related activities and efforts. To determine what progress DHS has made in implementing its mission functions and what work, if any, remains, we identified 10 DHS functional areas, which we define as categories or areas of DHS's homeland security responsibilities. These functional areas are based on those areas we identified for DHS in our August 2007 report on DHS's progress in implementing its mission and management functions, and our analysis of DHS's QHSR and budget documents, such as its congressional budget justifications.[8] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical

[6] DHS, *Bottom-Up Review Report* (Washington, D.C.: July 2010). As a result of the BUR, DHS acknowledged that it had complementary department responsibilities and capabilities, which it subsequently formalized in a sixth mission published in the fiscal year 2010-2012 Annual Performance Report—"Providing Essential Support to National and Economic Security"—to fully capture the scope of DHS's missions.

[7] GAO, *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*, GAO-11-881 (Washington, D.C.: Sept. 7, 2011).

[8] GAO-07-454.

assets; (4) surface transportation security; (5) border security; (6) maritime security; (7) immigration enforcement; (8) immigration services; (9); critical infrastructure protection—cyber assets; and (10) emergency preparedness and response.[9] To identify sub-areas within these functional areas, we identified performance expectations, which we define as composites of the responsibilities or functions that the department is to achieve or satisfy based on our analysis of requirements, responsibilities, and goals set for the department by Congress, the administration, and DHS itself and its components. In particular, we used expectations identified in our August 2007 report as a baseline, and updated, or added to, these expectations by analyzing requirements and plans set forth in homeland security-related laws, presidential directives and executive orders, national strategies, and DHS's and components' strategic plans and documents. We then aligned our functional areas to the five QHSR missions based on our review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents.

To identify key areas of progress and work that remains in each functional area, as well as crosscutting issues that have affected DHS's implementation efforts, we examined our and the DHS IG's past reports. We selected key work that we and the DHS IG have completed related to the functional areas, sub-areas, and crosscutting issues. We examined the methodologies used by the DHS IG in its reports, including reviewing the scope, methodological steps, and limitations. We determined that the DHS IG reports were sufficiently reliable for the purposes of our report to provide examples of, and to supplement our work on, DHS's progress and work remaining. We identified crosscutting issues based on analysis of our work in each functional mission area to determine common themes that have affected DHS's implementation efforts across the various mission areas. We conducted this performance audit from April 2011 through September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan

[9] We focused these mission areas primarily on DHS's homeland security-related functions. We did not consider the Secret Service, domestic counterterrorism or intelligence activities because (1) we and the DHS IG have completed limited work in these areas; (2) there are few, if any, requirements identified for the Secret Service's mission and for DHS's role in domestic counterterrorism and intelligence (the Department of Justice serves as the lead agency for most counterterrorism initiatives); and (3) we address DHS actions that could be considered part of domestic counterterrorism and intelligence in other areas, such as aviation security, critical infrastructure protection, and border security.

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.

In commenting on our September 2011 report, DHS acknowledged our work to assess the progress the department has made in enhancing the nation's security and the challenges that still exist. The department discussed its views of its accomplishments since 2001, such as the creation and management of the Visa Security Program; the establishment of fusion centers to serve as focal points for the analysis and sharing on threat and vulnerability-related information; and passenger screening and prescreening programs, among other things. We recognize the department's progress in these and other areas in the report, as well as identify existing challenges that will be important for DHS to address moving forward. DHS further noted that the report did not address all of DHS's homeland security-related activities and efforts. DHS also stated that the report's assessments of progress in each homeland security mission area were not comprehensive because we and the DHS IG completed varying degrees of work for each area. We reflect in the report that it was primarily based on work we completed since DHS began operations, supplemented with the work of the DHS IG, with an emphasis on work completed since 2008 and updated information provided by DHS in July and August 2011. As such, the report identified that our work and that of the DHS IG did not cover all of DHS's homeland security-related programs and activities, and that the report was not intended to do so. Further, we noted in the report that because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each functional area, and because different DHS components and offices provided us with different amounts and types of information, the report's assessments of DHS's progress in each area reflected the information available for our review and analysis and were not necessarily equally comprehensive across all 10 areas.

DHS Continues to Implement and Strengthen Its Mission Functions, but Key Operational and Management Challenges Remain

Since DHS began operations in March 2003, it has developed and implemented key policies, programs, and activities for implementing its homeland security missions and functions that have created and strengthened a foundation for achieving its potential as it continues to mature. However, the department's efforts have been hindered by challenges faced in leading and coordinating the homeland security enterprise; implementing and integrating its management functions for results; and strategically managing risk and assessing, and adjusting as necessary, its homeland security efforts.[10] DHS has made progress in these three areas, but needs to take additional action, moving forward, to help it achieve its full potential.

DHS Has Made Progress in Implementing its Mission Functions, but Program Weaknesses and Management Issues Have Hindered Implementation Efforts

DHS has made important progress in implementing and strengthening its mission functions over the past 8 years, including implementing key homeland security operations and achieving important goals and milestones in many areas. The department's accomplishments include developing strategic and operational plans across its range of missions; hiring, deploying and training workforces; establishing new, or expanding existing, offices and programs; and developing and issuing policies, procedures, and regulations to govern its homeland security operations. For example:

- DHS issued the QHSR, which provides a strategic framework for homeland security, and the National Response Framework, which outlines guiding principles for disaster response.
- DHS successfully hired, trained, and deployed workforces, such as a federal screening workforce which assumed security screening responsibilities at airports nationwide, and the department has about 20,000 agents to patrol U.S. land borders.
- DHS created new programs and offices, or expanded existing ones, to implement key homeland security responsibilities, such as establishing the United States Computer Emergency Readiness Team to, among other things, coordinate the nation's

[10] DHS defines the homeland security enterprise as the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities, who share a common national interest in the safety and security of the United States and its population.

efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. DHS also expanded programs for identifying and removing aliens subject to removal from the United States and for preventing unauthorized aliens from entering the country.

- DHS issued policies and procedures addressing, among other things, the screening of passengers at airport checkpoints, inspecting travelers seeking entry into the United States, and assessing immigration benefit applications and processes for detecting possible fraud.

Establishing these elements and others are important accomplishments and have been critical for the department to position and equip itself for fulfilling its homeland security missions and functions.

However, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. For example, we have reported that many DHS programs and investments have experienced cost overruns, schedule delays, and performance problems, including, for instance, DHS's recently cancelled technology program for securing U.S. borders, known as the Secure Border Initiative Network, and some technologies for screening passengers at airport checkpoints. Further, with respect to the cargo advanced automated radiography system to detect certain nuclear materials in vehicles and containers at ports DHS pursued the acquisition and deployment of the system without fully understanding that it would not fit within existing inspection lanes at ports of entry. DHS subsequently canceled the program. DHS also has not yet fully implemented its roles and responsibilities for developing and implementing key homeland security programs and initiatives. For example, DHS has not yet developed a set of target capabilities for disaster preparedness or established metrics for assessing those capabilities to provide a framework for evaluating preparedness, as required by the Post-Katrina Emergency Management Reform Act.[11] Our work has shown that DHS should take additional action to improve the efficiency and effectiveness of a number of its programs and activities by, for example, improving

[11] See 6 U.S.C. § 749.

program management and oversight, and better assessing homeland security requirements, needs, costs, and benefits, such as those for key acquisition and technology programs. Table 1 provides examples of key progress and work remaining in DHS's functional mission areas, with an emphasis on work we completed since 2008.

Table 1: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We and the DHS IG Have Reported

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 1: Preventing Terrorism and Enhancing Security	Aviation security	**Key progress:** DHS enhanced aviation security in key areas related to passenger prescreening, passenger checkpoint screening, checked baggage screening, and air cargo security. For example, DHS developed and implemented Secure Flight as a passenger prescreening program to match airline passenger information against terrorist watchlist records. DHS also deployed technology to screen passengers and checked baggage at airports. For example, in response to the December 25, 2009, attempted attack on Northwest flight 253, DHS revised the advanced imaging technology procurement and deployment strategy, increasing the planned deployment of advanced imaging technology from 878 to between 1,350 and 1,800 units.[a] Further, DHS is screening passengers using staff trained in behavior detection principles and deployed about 3,000 Behavior Detection Officers to 161 airports as part of its Screening of Passengers by Observation Techniques program. Moreover, DHS reported, as of August 2010, that it had established a system to screen 100 percent of domestic air cargo (cargo transported within and outbound from the United States) transported on passenger aircraft by, among other things, creating a voluntary program to facilitate screening throughout the air cargo supply chain and taking steps to test technologies for screening air cargo. **What remains to be done:** DHS should take additional action to strengthen its aviation security efforts. For example, a risk-based strategy and a cost-benefit analysis of airport checkpoint technologies would improve passenger checkpoint screening. TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based and did not reflect some of the key risk management principles, such as conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and did not include a cost-benefit analysis and performance measures. Further, in March 2010, we reported that it was unclear whether the advanced imaging technology would have detected the weapon used in the December 25, 2009 attempted terrorist attack based on the preliminary testing information we received. DHS also had not validated the science supporting its Screening of Passengers by Observation Techniques program, or determined if behavior detection techniques could be successfully used across the aviation system to detect threats before deploying the program. DHS completed a program validation study in April 2011 which found that the program was more effective than random screening, but that more work was needed to determine whether the science could be used for counterterrorism purposes in the aviation environment. Moreover, DHS does not yet have a plan and schedule for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements. In addition, DHS does not yet have a mechanism to verify the accuracy of domestic and inbound air cargo screening data to help ensure that screening is being conducted at reported levels, and DHS does not yet have approved technology to screen cargo once it is loaded onto a pallet or container—both of which are common means of transporting air cargo on passenger aircraft, thus requiring that screening occur before incorporation into pallets and containers.

QHSR mission	Functional area	Summary of key progress and work remaining
	CBRN threats	**Key progress:** DHS made progress in assessing risks posed by CBRN threats, developing CBRN detection capabilities, and planning for nuclear detection. For example, DHS develops risk assessments of CBRN threats and has issued seven classified CBRN risk assessments since 2006. DHS also assessed the threat posed by specific CBRN agents in order to determine which of those agents pose a material threat to the United States, known as material threat assessments. With regard to CBRN detection capabilities, DHS implemented the BioWatch program in more than 30 metropolitan areas to detect specific airborne biological threat agents. Further, DHS established the National Biosurveillance Integration Center to enhance the federal government's capability to identify and track biological events of national concern. In addition, DHS coordinated the development of a strategic plan for the global nuclear detection architecture—a multidepartment effort to protect against terrorist attacks using nuclear and radiological materials through coordinated activities—and has deployed radiation detection equipment. **What remains to be done:** More work remains for DHS to strengthen its CBRN assessment, detection, and mitigation capabilities. For example, DHS should better coordinate with the Department of Health and Human Services in conducting CBRN risk assessments by developing written policies and procedures governing development of the assessments. Moreover, the National Biosurveillance Integration Center lacks resources necessary for operations, such as data and personnel from its partner agencies. Additionally, work remains for DHS in its implementation of the global nuclear detection architecture. Specifically, the strategic plan for the architecture did not include some key components, such as funding needed to achieve the strategic plan's objectives, or monitoring mechanisms for determining programmatic progress and identifying needed improvements. DHS officials told us that they will address these missing elements in an implementation plan, which they plan to issue by the end of 2011.

QHSR mission	Functional area	Summary of key progress and work remaining
	Critical infrastructure protection – physical assets	**Key progress:** DHS expanded its efforts to conduct risk assessment and planning, provide for protection and resiliency, and implement partnerships and coordination mechanisms for physical critical assets. For example, DHS updated the National Infrastructure Protection Plan to include an emphasis on resiliency (the capacity to resist, absorb, or successfully adapt, respond to, or recover from disasters), and enhanced discussion about DHS risk management. Moreover, DHS components with responsibility for critical infrastructure sectors, such as transportation security, have begun to use risk-based assessments in their critical infrastructure related planning and protection efforts. Further, DHS has various voluntary programs in place to conduct vulnerability assessments and security surveys at and across facilities from the 18 critical infrastructure sectors, and uses these assessments to develop and disseminate information on steps asset owners and operators can take to protect their facilities. In addition, DHS coordinated with critical infrastructure stakeholders, including other federal regulatory authorities to identify overlaps and gaps in critical infrastructure security activities. **What remains to be done:** Additional actions are needed for DHS to strengthen its critical infrastructure protection programs and efforts. For example, DHS has not fully implemented an approach to measure its effectiveness in working with critical asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during various vulnerability assessments. Moreover, DHS components have faced difficulties in incorporating risk-based assessments in critical infrastructure planning and protection efforts, such as in planning for security in surface transportation modes like freight rail and highway infrastructure. Further, DHS should determine the feasibility of developing an approach to disseminating information on resiliency practices to its critical infrastructure partners to better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments.
	Surface transportation security	**Key progress:** DHS expanded its efforts in key surface transportation security areas, such as risk assessments and strategic planning; the surface transportation inspector workforce; and information sharing. For example, DHS conducted risk assessments of surface transportation modes and developed a transportation sector security risk assessment that assessed risk within and across the various modes. Further, DHS more than doubled its surface transportation inspector workforce and, as of July 2011, reported that its surface inspectors had conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, among other things. Moreover, DHS allocates transit grant funding based on risk assessments and has taken steps to measure performance of its Transit Security Grant Program, which provides funds to owners and operators of mass transit and passenger rail systems. In addition, DHS expanded its sharing of surface transportation security information by establishing information networks. **What remains to be done:** DHS should take further action to strengthen its surface transportation security programs and operations. For example, DHS's efforts to improve elements of risk assessments of surface transportation modes are in the early stages of implementation. Moreover, DHS noted limitations in its transportation sector security risk assessment—such as the exclusion of threats from "lone wolf" operators—that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. Further, DHS has not yet completed a long-term workforce plan that identifies future needs for its surface inspector workforce. It also has not yet issued regulations for a training program for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[b] Additionally, DHS's information sharing efforts would benefit from improved streamlining, coordination, and assessment of the effectiveness of information sharing mechanisms.

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 2: Securing and Managing Our Borders	Border security	**Key progress:** DHS expanded its efforts in key border security areas, such as inspection of travelers and cargo at ports of entry, security of the border between ports of entry, visa adjudication security, and collaboration with stakeholders. Specifically, DHS has undertaken efforts to keep terrorists and other dangerous people from entering the country. For example, DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information. DHS established plans for, and had begun to interact with and involve stakeholders in, developing an exit capability. DHS deployed technologies and other infrastructure to secure the border between ports of entry, including more than 600 miles of tactical infrastructure, such as fencing, along the border. DHS also deployed the Visa Security Program, in which DHS personnel review visa applications to help prevent individuals who pose a threat from entering the United States, to 19 posts in 15 countries, and developed a 5-year expansion plan for the program. In addition, DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts through, among other things, the establishment of interagency forums. **What remains to be done:** More work remains for DHS to strengthen its border security programs and operations. For example, although it has developed a plan, DHS has not yet adopted an integrated approach to scheduling, executing, and tracking the work needed to be accomplished to deliver a comprehensive biometric exit solution as part of the US-VISIT program. Further, DHS experienced schedule delays and performance problems with its information technology program for securing the border between ports of entry—the Secure Border Initiative Network—which led to its cancellation. Because of the program's decreased scope, uncertain timing, unclear costs, and limited life cycle management, it was unclear whether DHS's pursuit of the program was cost-effective. DHS is transitioning to a new approach for border technology, which we are assessing. With regard to the Visa Security Program, DHS did not fully follow or update its 5-year expansion plan. For instance, it did not establish 9 posts identified for expansion in 2009 and 2010, and had not taken steps to address visa risk at posts that did not have a Visa Security Program presence. Additionally, DHS should strengthen its oversight of interagency forums operating along the northern border.

QHSR mission	Functional area	Summary of key progress and work remaining
	Maritime security	**Key progress:** DHS expanded its efforts in key maritime security areas, such as port facility and vessel security, maritime security domain awareness and information sharing, and international supply chain security. For example, DHS strengthened risk management through the development of a risk assessment model, and addressed risks to port facilities through annual inspections in which DHS identified and corrected deficiencies, such as facilities failing to follow security plans for access control. Further, DHS took action to address risks posed by foreign seafarers entering U.S. seaports by, for example, conducting advance-screening before the arrival of vessels at U.S. ports, inspections, and enforcement operations. DHS developed the Transportation Worker Identification Credential program to manage the access of unescorted maritime workers to secure areas of regulated maritime facilities. DHS also implemented measures to help secure passenger vessels including cruise ships, ferries, and energy commodity vessels such as tankers, such as assessing risks to these types of vessels. Moreover, for tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system, and a commercially provided long-range automatic identification system. For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system, and also either operates, or has access to, radar and cameras in some ports. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments. **What remains to be done:** DHS should take additional action to strengthen its maritime security efforts. For example, because of a lack of technology capability, DHS did not electronically verify identity and immigration status of foreign seafarers, as part of its onboard admissibility inspections of cargo vessels, thus limiting the assurance that fraud could be identified among documents presented by them. In addition, the Transportation Worker Identification Credential program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Moreover, DHS has not assessed the costs and benefits of requiring cruise lines to provide passenger reservation data for screening, which could help improve identification and targeting of potential terrorists. Further, the vessel tracking systems used in U.S. coastal areas, inland waterways, and ports had more difficulty tracking smaller and noncommercial vessels because these vessels were not generally required to carry automatic identification system equipment, and because of the technical limitations of radar and cameras. In addition, DHS has made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative, a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas, leaving the feasibility of 100 percent scanning largely unproven. CBP has not yet developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.[c]

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 3: Enforcing and Administering Our Immigration Laws	Immigration enforcement	**Key progress:** DHS expanded its immigration and customs enforcement programs and activities in key areas such as overstay enforcement, compliance with workplace immigration laws, alien smuggling, and firearms trafficking. For example, DHS increased its resources for investigating overstays (unauthorized immigrants who entered the United States legally on a temporary basis then overstayed their authorized periods of admission) and alien smuggling operations, and deployed border enforcement task forces to investigate illicit smuggling of people and goods, including firearms. In addition, DHS took action to improve the E-Verify program, which provides employers a voluntary tool for verifying an employee's authorization to work in the United States, by, for example, increasing the program's accuracy by expanding the number of databases it can query. Further, DHS expanded its programs and activities to identify and remove criminal aliens in federal, state, and local custody who are eligible for removal from the United States by, for example, entering into agreements with state and local law enforcement agencies to train officers to assist in identifying those individuals who are in the United States illegally. **What remains to be done:** Key weaknesses remain in DHS's immigration and customs enforcement efforts. For example, DHS took action to address a small portion of the estimated overstay population in the United States, and lacks measures for assessing its progress in addressing overstays. In particular, DHS field offices had closed about 34,700 overstay investigations assigned to them from fiscal year 2004 through 2010, as of October 2010; these cases resulted in approximately 8,100 arrests, relative to a total estimated overstay population of 4 million to 5.5 million.[d] Additionally, we reported that since fiscal year 2006, U.S. Immigration and Customs Enforcement within DHS allocated about 3 percent of its investigative work hours to overstay investigations Moreover, DHS should better leverage opportunities to strengthen its alien smuggling enforcement efforts by assessing the possible use of various investigative techniques, such as those to follow cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. Further, weaknesses with the E-Verify program, including challenges in accurately estimating E-Verify costs, put DHS at an increased risk of not making informed investment decisions.

QHSR mission	Functional area	Summary of key progress and work remaining
	Immigration services	**Key progress:** DHS improved the quality and efficiency of the immigration benefit administration process, and expanded its efforts to detect and deter immigration fraud. For example, DHS initiated efforts to modernize its immigration benefit administration infrastructure; improve the efficiency and timeliness of its application intake process; and ensure quality in its benefit adjudication processes. Further, DHS designed training programs and quality reviews to help ensure the integrity of asylum adjudications. Moreover, in 2004 DHS established the Office of Fraud Detection and National Security, now a directorate, to lead immigration fraud detection and deterrence efforts, and this directorate has since developed and implemented strategies for this purpose. **What remains to be done:** More work remains in DHS's efforts to improve its administration of immigration benefits. For example, DHS's program for transforming its immigration benefit processing infrastructure and business practices from paper-based to digital systems missed its planned milestones by more than 2 years, and has been hampered by management challenges, such as insufficient planning and not adhering to DHS acquisition guidance before selecting a contractor to assist with implementation of the transformation program. Additionally, while the Fraud Detection and National Security Directorate put in place strategies for detecting and deterring immigration fraud, DHS should take additional action to address vulnerabilities identified in its assessments intended to determine the extent and nature of fraud in certain applications. Further, despite mechanisms DHS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers we surveyed cited challenges in identifying fraud as a key factor affecting their adjudications. For example, 73 percent of asylum officer survey respondents reported it was moderately or very difficult to identify document fraud.

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 4: Safeguarding and Securing Cyberspace	Critical infrastructure protection – cyber assets	**Key progress:** DHS expanded its efforts to conduct cyber security risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cyber security partnerships and coordination mechanisms. For example, DHS developed the first National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels. DHS also took steps to secure external network connections in use by the federal government by establishing the National Cybersecurity Protection System, operationally known as Einstein, to analyze computer network traffic information to and from agencies. In 2008, DHS developed Einstein 2, which incorporated network intrusion detection technology into the capabilities of the initial version of the system. Additionally, the department made progress in enhancing its cyber analysis and incident warning capabilities through the establishment of the U.S. Computer Emergency Readiness Team, which, among other things, coordinates the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. Moreover, since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing lessons it had learned from this exercise to strengthen public and private incident response capabilities. **What remains to be done:** Key challenges remain in DHS's cyber security efforts. For example, to expand its protection and resiliency efforts, DHS needs to lead a concerted effort to consolidate and better secure Internet connections at federal agencies. Further, DHS faced challenges regarding deploying Einstein 2, including understanding the extent to which its objective was being met because the department lacked performance measures that addressed whether agencies report whether the alerts represent actual incidents. DHS also faces challenges in fully establishing a comprehensive national cyber analysis and warning capability. For example, the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. These attributes are related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, the U.S. Computer Emergency Readiness Team provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Additionally, expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 5: Ensuring Resilience to Disasters	Emergency preparedness and response	**Key progress:** DHS expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; and enhanced emergency communications. For example, DHS developed various plans for disaster preparedness and response. In particular, in 2004 DHS issued the National Response Plan and subsequently made revisions to it, culminating in the issuance of the National Response Framework in January 2008, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for response to disasters of all sizes and causes. Further, DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-based preparedness, and a Target Capabilities List, designed to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS also assisted local communities with developing long-term disaster recovery plans as part of its post-disaster assistance. For example, DHS assisted Iowa City's recovery from major floods in 2008 by, among other things, identifying possible federal funding sources for specific projects in the city's recovery plan, and advising the city on how to prepare effective project proposals. DHS is also finalizing a National Disaster Recovery Framework, intended to provide a model to identify and address challenges that arise during the disaster recovery process. Moreover, DHS issued the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide. **What remains to be done:** More work remains in DHS's efforts to establish and assess capabilities to define all hazards and provide long-term disaster recovery assistance. For example, DHS has not yet developed national preparedness capability requirements based on established metrics to provide a framework for assessing preparedness. Further, the data DHS collected to measure national preparedness were limited by reliability and measurement issues related to the lack of standardization. Until a framework for assessing preparedness is in place, DHS will not have a basis on which to operationalize and implement its conceptual approach for assessing local, state, and federal preparedness capabilities against capability requirements and identify capability gaps for prioritizing investments in national preparedness. Moreover, with regard to long-term disaster recovery assistance, DHS's criteria for when to provide the assistance were vague, and, in some cases, DHS provided assistance before state and local governments had the capacity to work effectively with DHS. Additionally, DHS should improve the efficacy of the grant application and review process by mitigating duplication or redundancy within the various preparedness grant programs. Until DHS evaluates grant applications across grant programs, DHS cannot ascertain whether or to what extent multiple funding requests are being submitted for similar purposes.

Source: GAO analysis based on the areas included in our September 2011 report.

[a] Advanced imaging technology units produce an image of a passenger's body that DHS personnel use to look for anomalies, such as explosives or other prohibited items.

[b] The Implementing Recommendations of the 9/11 Commission Act requires TSA to issue regulations for a training program to prepare mass transit, rail, and over-the-road bus employees for potential security threats and conditions. 6 U.S.C. §§ 1137, 1167, 1184.

[c] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-490 (2007) (amending 6 U.S.C. § 982(b)).

[d] According to our April 2011 report, the most recent estimates from the Pew Hispanic Center approximated that, in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays. Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, D.C.: May 22, 2006).

Impacting the department's ability to efficiently and effectively satisfy its missions are: (1) the need to integrate and strengthen its management functions; (2) the need for increased utilization of performance assessments; (3) the need for an enhanced use of risk information to inform planning, programming, and investment decision-making; (4) limitations in effective sharing and use of terrorism-related information; (5) partnerships that are not sustained or fully leveraged; and (6) limitations in developing and deploying technologies to meet mission needs. DHS made progress in addressing these areas, but more work is needed, going forward, to further mitigate these challenges and their impact on DHS's mission implementation.

For instance, DHS strengthened its performance measures in recent years and linked its measures to the QHSR's missions and goals. However, DHS and its components have not yet developed measures for assessing the effectiveness of key homeland security programs, such as programs for securing the border and preparing the nation for emergency incidents. For example, with regard to checkpoints DHS operates on U.S. roads to screen vehicles for unauthorized aliens and contraband, DHS established three performance measures to report the results of checkpoint operations. However, the measures did not indicate if checkpoints were operating efficiently and effectively and data reporting and collection challenges hindered the use of results to inform Congress and the public on checkpoint performance. Moreover, DHS has not yet established performance measures to assess the effectiveness of its programs for investigating alien smuggling operations and foreign nationals who overstay their authorized periods of admission to the United States, making it difficult for these agencies to determine progress made in these areas and evaluate possible improvements.

Further, DHS and its component agencies developed strategies and tools for conducting risk assessments. For example, DHS has conducted risk assessments of various surface transportation modes, such as freight rail, passenger rail, and pipelines. However, the department needs to strengthen its use of risk information to inform its planning and investment decision-making. For example, DHS could better use risk information to plan and prioritize security measures and investments within and across its mission areas, as the department cannot secure the nation against every conceivable threat.

In addition, DHS took action to develop and deploy new technologies to help meet its homeland security missions. However, in a number of instances DHS pursued acquisitions without ensuring that the

technologies met defined requirements, conducting and documenting appropriate testing and evaluation, and performing cost-benefit analyses, resulting in important technology programs not meeting performance expectations. For example, in 2006, we recommended that DHS's decision to deploy next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials, be based on an analysis of both the benefits and costs and a determination of whether any additional detection capability provided by the portals was worth their additional cost. DHS subsequently issued a cost-benefit analysis, but we reported that this analysis did not provide a sound analytical basis for DHS's decision to deploy the portals. In June 2009, we also reported that an updated cost-benefit analysis might show that DHS's plan to replace existing equipment with advanced spectroscopic portals was not justified, particularly given the marginal improvement in detection of certain nuclear materials required of advanced spectroscopic portals and the potential to improve the current-generation portal monitors' sensitivity to nuclear materials, most likely at a lower cost. In July 2011, DHS announced that it would end the advanced spectroscopic portal project as originally conceived given the challenges the program faced.

As we have previously reported, while it is important that DHS continue to work to strengthen each of its functional areas, it is equally important that these areas be addressed from a comprehensive, departmentwide perspective to help mitigate longstanding issues that have impacted the department's progress.

Key Themes Have Impacted DHS's Progress in Implementing Its Mission Functions

Our work at DHS has identified several key themes—leading and coordinating the homeland security enterprise, implementing and integrating management functions for results, and strategically managing risks and assessing homeland security efforts—that have impacted the department's progress since it began operations. These themes provide insights that can inform DHS's efforts, moving forward, as it works to implement its missions within a dynamic and evolving homeland security environment. DHS made progress and has had successes in all of these areas, but our work found that these themes have been at the foundation of DHS's implementation challenges, and need to be addressed from a departmentwide perspective to position DHS for the future and enable it to satisfy the expectations set for it by the Congress, the administration, and the country.

Leading and coordinating the homeland security enterprise. While DHS is one of a number of entities with a role in securing the homeland, it has significant leadership and coordination responsibilities for managing efforts across the homeland security enterprise. To satisfy these responsibilities, it is critically important that DHS develop, maintain and leverage effective partnerships with its stakeholders, while at the same time addressing DHS-specific responsibilities in satisfying its missions. Before DHS began operations, we reported that the quality and continuity of the new department's leadership would be critical to building and sustaining the long-term effectiveness of DHS and achieving homeland security goals and objectives. We further reported that to secure the nation, DHS must form effective and sustained partnerships between components and also with a range of other entities, including federal agencies, state and local governments, the private and nonprofit sectors, and international partners.

DHS has made important strides in providing leadership and coordinating efforts. For example, it has improved coordination and clarified roles with state and local governments for emergency management. DHS also strengthened its partnerships and collaboration with foreign governments to coordinate and standardize security practices for aviation security. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, we reported that the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. Without improvements in meeting private and public sector expectations for sharing cyber threat information, private-public partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the information and mechanisms needed to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure. Moreover, we reported that DHS needs to continue to streamline its mechanisms for sharing information with public transit agencies to reduce the volume of similar information these agencies receive from DHS, making it easier for them to discern relevant information and take appropriate actions to enhance security.

In 2005, we designated information sharing for homeland security as high risk because the federal government faced serious challenges in analyzing information and sharing it among partners in a timely, accurate, and useful way. Gaps in sharing, such as agencies' failure to link

information about the individual who attempted to conduct the December 25, 2009, airline bombing, prevented the individual from being included on the federal government's consolidated terrorist watchlist, a tool used by DHS to screen for persons who pose a security risk. The federal government and DHS have made progress, but more work remains for DHS to streamline its information sharing mechanisms and better meet partners' needs. Moving forward, it will be important that DHS continue to enhance its focus and efforts to strengthen and leverage the broader homeland security enterprise, and build off the important progress that it has made thus far. In addressing ever-changing and complex threats, and with the vast array of partners with which DHS must coordinate, continued leadership and stewardship will be critical in achieving this end.

Implementing and integrating management functions for results. Following its establishment, the department focused its efforts primarily on implementing its various missions to meet pressing homeland security needs and threats, and less on creating and integrating a fully and effectively functioning department from 22 disparate agencies. This initial focus on mission implementation was understandable given the critical homeland security needs facing the nation after the department's establishment, and the enormous challenge posed by creating, integrating, and transforming a department as large and complex as DHS. As the department matured, it has put into place management policies and processes and made a range of other enhancements to its management functions—acquisition, information technology, financial, and human capital management. However, DHS has not always effectively executed or integrated these functions. In 2003, we designated the transformation and integration of DHS as high risk because DHS had to transform 22 agencies 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. Eight years later, DHS remains on our high-risk list. DHS has demonstrated strong leadership commitment to addressing its management challenges and has begun to implement a strategy to do so. Further, DHS developed various management policies, directives, and governance structures, such as acquisition and information technology management policies and controls, to provide enhanced guidance on investment decision making. DHS also reduced its financial management material weaknesses in internal control over financial reporting and developed strategies to strengthen human capital management, such as its *Workforce Strategy for Fiscal Years 2011-2016*.

However, DHS needs to continue to demonstrate sustainable progress in addressing its challenges, as these issues have contributed to schedule delays, cost increases, and performance problems in major programs aimed at delivering important mission capabilities. For example, in September 2010, we reported that the Science and Technology Directorate's master plans for conducting operational testing of container security technologies did not reflect all of the operational scenarios that U.S. Customs and Border Protection was considering for implementation. In addition, when it developed the US-VISIT program, DHS did not sufficiently define what capabilities and benefits would be delivered, by when, and at what cost, and the department has not yet determined how to deploy a biometric exit capability under the program. Moreover, DHS does not yet have enough skilled personnel to carry out activities in various areas, such as acquisition management; and has not yet implemented an integrated financial management system, impacting its ability to have ready access to reliable, useful, and timely information for informed decision making. Moving forward, addressing these management challenges will be critical for DHS's success, as will be the integration of these functions across the department to achieve efficiencies and effectiveness.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats, such as attempted attacks against the aviation sector, have impacted and altered DHS's approaches and investments, such as changes DHS made to its processes and technology investments for screening passengers and baggage at airports. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs or not doing so in an efficient manner. For example, as we reported in July 2011, the Coast Guard's planned acquisitions through its Deepwater Program, which began before DHS's creation and includes efforts to build or modernize ships and aircraft and supporting capabilities that are critical to meeting the Coast Guard's core missions in the future, is unachievable due to cost growth, schedule delays and affordability issues. In addition, because FEMA has not yet developed a set of target disaster preparedness capabilities and a systematic means of assessing those capabilities, as required by the Post-Katrina Emergency Management Reform Act and Presidential Policy Directive 8, it cannot

effectively evaluate and identify key capability gaps and target limited resources to fill those gaps.

Further, DHS has made important progress in analyzing risk across sectors, but it has more work to do in using this information to inform planning and resource allocation decisions. Risk management has been widely supported by Congress and DHS as a management approach for homeland security, enhancing the department's ability to make informed decisions and prioritize resource investments. Since DHS does not have unlimited resources and cannot protect the nation from every conceivable threat, it must make risk-informed decisions regarding its homeland security approaches and strategies.

Moreover, we have reported on the need for enhanced performance assessment, that is, evaluating existing programs and operations to determine whether they are operating as intended or are in need of change, across DHS's missions. Information on the performance of programs is critical for helping the department, Congress, and other stakeholders more systematically assess strengths and weaknesses and inform decision making. In recent years, DHS has placed an increased emphasis on strengthening its mechanisms for assessing the performance and effectiveness of its homeland security programs. For example, DHS established new performance measures, and modified existing ones, to better assess many of its programs and efforts.

However, our work has found that DHS continues to miss opportunities to optimize performance across its missions because of a lack of reliable performance information or assessment of existing information; evaluation among feasible alternatives; and, as appropriate, adjustment of programs or operations that are not meeting mission needs. For example, DHS's program for research, development, and deployment of passenger checkpoint screening technologies lacked a risk-based plan and performance measures to assess the extent to which checkpoint screening technologies were achieving the program's security goals, and thereby reducing or mitigating the risk of terrorist attacks. As a result, DHS had limited assurance that its strategy targeted the most critical risks and that it was investing in the most cost-effective new technologies or other protective measures. As the department further matures and seeks to optimize its operations, DHS will need to look beyond immediate requirements; assess programs' sustainability across the long term, particularly in light of constrained budgets; and evaluate tradeoffs within and among programs across the homeland security enterprise. Doing so

should better equip DHS to adapt and respond to new threats in a sustainable manner as it works to address existing ones.

Concluding Observations

Given DHS's role and leadership responsibilities in securing the homeland, it is critical that the department's programs and activities are operating as efficiently and effectively as possible, are sustainable, and continue to mature, evolve and adapt to address pressing security needs. DHS has made significant progress throughout its missions since its creation, but more work is needed to further transform the department into a more integrated and effective organization. DHS has also made important progress in strengthening partnerships with stakeholders, improving its management processes and sharing of information, and enhancing its risk management and performance measurement efforts. These accomplishments are especially noteworthy given that the department has had to work to transform itself into a fully functioning cabinet department while implementing its missions—a difficult undertaking for any organization and one that can take years to achieve even under less daunting circumstances.

Impacting the department's efforts have been a variety of factors and events, such as attempted terrorist attacks and natural disasters, as well as new responsibilities and authorities provided by Congress and the administration. These events collectively have forced DHS to continually reassess its priorities and reallocate resources as needed, and have impacted its continued integration and transformation. Given the nature of DHS's mission, the need to remain nimble and adaptable to respond to evolving threats, as well as to work to anticipate new ones, will not change and may become even more complex and challenging as domestic and world events unfold, particularly in light of reduced budgets and constrained resources. To better position itself to address these challenges, our work has shown that DHS should place an increased emphasis and take additional action in supporting and leveraging the homeland security enterprise, managing its operations to achieve needed results, and strategically planning for the future while assessing and adjusting, as needed, what exists today. Addressing these issues will be critically important for the department to strengthen its homeland security programs and operations. Eight years after its establishment and 10 years after the September 11, 2001, terrorist attacks, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Rebecca Gambler, Assistant Director; Melissa Bogar; Susan Czachor; Sarah Kaczmarek; Tracey King; Taylor Matheson; Jessica Orr; and Meghan Squires.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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