United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2011

DEPARTMENT OF HOMELAND SECURITY

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

U.S. Government Accountability Office

GAO 90 YEARS 1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

GAO-11-881

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-881, a report to congressional requesters

September 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 events of September 11, 2001, led to profound changes in government policies and structures to confront homeland security threats. 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, 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 report addresses DHS's progress in implementing its homeland security missions since it began operations, work remaining, and issues affecting implementation efforts. This report is based on GAO's past and ongoing work, supplemented with DHS Office of Inspector General reports, with an emphasis on reports issued since 2008. GAO also analyzed information provided by DHS in July and August 2011 on recent actions taken in response to prior work.

What GAO Recommends

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

View GAO-11-881 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, and awards preparedness grants based on a reasonable risk methodology. 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 a number of programs aimed at delivering important mission capabilities, such as a system to detect certain nuclear materials in vehicles and containers at ports. DHS also faced difficulties in deploying some technologies that meet defined requirements. Further, DHS does not yet have enough skilled personnel 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.

Contents

Letter		1
	Background	10
	DHS Continues to Implement and Strengthen Its Mission Functions, but Key Operational and Management Challenges Remain	16
	Agency Comments and Our Evaluation	37
Appendix I	Department of Homeland Security Functional Mission Areas, Sub-Areas, and Performance Expectations	40
Appendix II	Scope and Methodology	47
Appendix III	Aviation Security	55
Appendix IV	Chemical, Biological, Radiological, and Nuclear Threats	66
Appendix V	Critical Infrastructure Protection—Physical Assets	72
Appendix VI	Surface Transportation Security	81
Appendix VII	Border Security	91
Appendix VIII	Maritime Security	103

Appendix IX	Immigration Enforcement	116
Appendix X	Immigration Services	123
Appendix XI	Critical Infrastructure Protection—Cyber Assets	130
Appendix XII	Emergency Preparedness and Response	140
Appendix XIII	Department of Homeland Security Transformation and Implementation	152
Appendix XIV	Performance Measurement	162
Appendix XV	Risk Management	167
Appendix XVI	Information Sharing	175
Appendix XVII	Partnerships and Coordination	181
Appendix XVIII	Developing and Deploying New Technologies for Homeland Security	186

Appendix XIX Comments from the Department of Homeland Security 192

Appendix XX GAO Contact and Staff Acknowledgments 197

Related Reports 198

Tables

Table 1: DHS Budget Authority for Fiscal Years 2004 through 2011 in Thousands of Dollars, as Reported by DHS 12
Table 2: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We Have Reported 199
Table 3: Crosscutting and Management Issues Affecting DHS's Progress in Implementing Its Homeland Security Missions 29
Table 4: DHS Functional Areas, Sub-Areas, and Performance Expectations 40
Table 5: Example of Performance Expectations and Sub-Areas for Border Security 49
Table 6: Alignment of Functional Areas under DHS's QHSR Missions 51
Table 7: Assessment of Progress and Work Remaining in Key Aviation Security Areas on Which We Have Reported 57
Table 8: Assessment of Progress and Work Remaining in Key CBRN Threats Areas on Which We Have Reported 68
Table 9: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection–Physical Assets Areas on Which We Have Reported 74
Table 10: Assessment of Progress and Work Remaining in Key Surface Transportation Security Areas on Which We Have Reported 83
Table 11: Assessment of Progress and Work Remaining in Key Border Security Areas on Which We Have Reported 93
Table 12: Assessment of Progress and Work Remaining in Key Maritime Security Areas on Which We Have Reported 106
Table 13: Assessment of Progress and Work Remaining in Key Immigration Enforcement Areas on Which We Have Reported 118

Table 14: Assessment of Progress and Work Remaining in Key Immigration Services Areas on Which We Have Reported 125
Table 15: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Cyber Assets Areas on Which We Have Reported 133
Table 16: Assessment of Progress and Work Remaining in Emergency Preparedness and Response on Which We Have Reported 142

Figures

Figure 1: Selected Events That Have Affected DHS Implementation Efforts 15
Figure 2: GAO Risk Management Framework 168
Figure 3: DHS Risk Management Framework 170

Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BUR	Bottom-Up Review
CBP	U.S. Customs and Border Protection
CBRN	chemical, biological, radiological, and nuclear
CS&C	Office of Cyber Security and Communications
CTCEU	Counterterrorism and Criminal Exploitation Unit
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
ICE	U.S. Immigration and Customs Enforcement
IG	Inspector General
NPPD	National Protection and Programs Directorate
QHSR	Quadrennial Homeland Security Review
S&T	Science and Technology Directorate
SBI	Secure Border Initiative
SBI*net*	Secure Border Initiative Network
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

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

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 7, 2011

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

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

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. Most notably, in the aftermath of the attacks, the Department of Homeland Security (DHS) was created 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. The 10-year anniversary of 9/11 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.[1]

The creation of DHS was an enormous management challenge, representing the fusion of 22 agencies, and the size, complexity, and

[1] We supplemented our work with selected work conducted by the Department of Homeland Security Office of Inspector General. This report highlights our work on key DHS programs and efforts, but neither addresses all products that we and the DHS Office of Inspector General issued related to DHS, nor addresses all of DHS's homeland security-related activities and efforts. Also, this report focuses on our work related to DHS's homeland security efforts; it does not address other federal agencies' homeland security efforts, such as the roles the Department of Defense and intelligence agencies play in homeland security and defense.

importance of the effort made the challenge especially daunting and critical to the nation's security.[2] DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. Since DHS began operations in March 2003, the department developed and refined the implementation of various policies and programs to address its homeland security missions as well as its nonhomeland security functions.[3] In particular, DHS implemented programs to secure the border and administer the immigration system; strengthen the security of the transportation sector; and prepare for and respond to terrorist threats and natural disasters. DHS also took actions to strengthen and better integrate its management functions and to transform its component agencies into a unified cabinet-level department.

We have evaluated numerous departmental programs and activities since DHS began its operations in 2003 and issued over 1,000 reports and congressional testimony in such areas as border security and immigration; transportation security; and emergency management, among others. We have made approximately 1,500 recommendations to DHS designed to improve its operations, such as to improve performance measurement efforts; strengthen management processes, including acquisition processes; enhance coordination and information sharing; and increase the use of risk information in planning and resource allocation decisions, as well as to address other key themes 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 much to do to ensure that it conducts its missions efficiently and effectively while simultaneously preparing to

[2] These 22 agencies, offices, and programs were U.S. Customs Service; U.S. Immigration and Naturalization Service; Federal Protective Service; Transportation Security Administration; Federal Law Enforcement Training Center; Animal and Plant Health Inspection Service; Office for Domestic Preparedness; Federal Emergency Management Agency; Strategic National Stockpile and the National Disaster Medical System; Nuclear Incident Response Team; Domestic Emergency Support Team; National Domestic Preparedness Office; Chemical, Biological, Radiological, and Nuclear Countermeasures Program; Environmental Measurement Laboratory; National BW Defense Analysis Center; Plum Island Animal Disease Center; Federal Computer Incident Response Center; National Communication System; National Infrastructure Protection Center; Energy Security and Assurance Program; Secret Service; and U.S. Coast Guard.

[3] Examples of nonhomeland security functions include trade enforcement and Coast Guard search and rescue. We are including DHS's missions related to administering immigration services in this report, as these efforts have a nexus to homeland security.

address future challenges that face the department and the nation. Addressing these challenges 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.[4] 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.[5] 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.[6] Most recently, in our 2011 high-risk update, we reported that DHS took action to implement, transform, and integrate its management functions, actions that directly affect its ability to meet its homeland security and other missions.[7] For example, senior leaders at the department, including the Secretary and Deputy Secretary of Homeland Security, demonstrated strong commitment and support to addressing this high-risk area by, among other things, designating the Under Secretary for Management to be responsible for coordinating DHS's efforts to address this high-risk area, as well as other senior officials to be responsible for implementing corrective actions within each

[4] 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.

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

[6] 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).

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

management function. Moreover, in January 2011 DHS developed a strategy for addressing existing integration and management issues and is in the early stages of its implementation. DHS provided an update to the strategy in June 2011 that detailed plans and status updates designed to integrate and strengthen its management functions. We plan to provide the department with feedback on this update later this year. Moving forward, we reported that DHS will need to continue to implement its high-risk strategy and efforts to identify and acquire resources needed to address its risks, monitor and validate its corrective actions, and show measurable, sustainable progress in achieving key outcomes. Demonstrated, sustainable progress will be critical to helping DHS strengthen and integrate management functions within and across the department and its components.

In February 2010, DHS issued its first Quadrennial Homeland Security Review (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.[8] 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 to the QHSR report, 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

[8] Department of Homeland Security, *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 of 2007 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.[9]

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.[10] We reported that DHS made progress in implementing all of its mission and management areas 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. Further, among its mission functions, we reported that in implementing expectations, DHS made substantial progress in maritime security; moderate progress in aviation and surface transportation security, critical infrastructure protection, and immigration enforcement; modest progress in border security and immigration services; and limited progress in emergency preparedness and response missions.[11] We also reported on various crosscutting issues related to areas such as risk management, partnerships and coordination, and performance measurement, that had impeded DHS's implementation efforts. We further noted that DHS generally had not established quantitative goals and measures for assessing its performance and as a result, we could not

[9] Department of Homeland Security, *Bottom-Up Review Report* (Washington, D.C.: July 2010). As a result of the BUR, DHS acknowledged 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, known as "Providing Essential Support to National and Economic Security," to fully capture the scope of DHS's missions.

[10] 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.

[11] We defined substantial progress as DHS taking action to generally achieve more than 75 percent of the identified performance expectations; moderate progress as DHS taking action to generally achieve more than 50 percent but 75 percent or less of the identified expectations; modest progress as DHS taking action to generally achieve more than 25 percent but 50 percent or less of the identified expectations; and limited progress as DHS taking action to generally achieve 25 percent or less of the identified expectations. We found that DHS generally achieved a performance expectation if our work showed that the department had taken actions to satisfy most of the key elements of the expectation but may not have satisfied all of the elements.

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. Further, at the request of the Senate Committee on Homeland Security and Governmental Affairs 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. Our feedback ranged from pointing out components' limited use of outcome-oriented performance measures to assess the results or effectiveness of programs, to raising questions about the steps taken by DHS or its components to ensure the reliability and verification of performance data. 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 QHSR missions and goals. The department plans to report on its results in meeting established targets for these new measures at the end of the fiscal year.

You asked us to review the progress made by DHS in implementing its homeland security missions since its creation after the September 11, 2001, terrorist attacks. This report addresses the following question: What progress has DHS made in implementing its mission functions since it began operations; what work, if any, remains; and what crosscutting and management issues have affected DHS's implementation efforts?

This report is based on our work on DHS since it began operations, and supplemented with work completed by the DHS Office of Inspector General (IG), with an emphasis on work completed since 2008, and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on key DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, we examined program documentation and interviewed agency officials, among other things. Our work and the work of the DHS IG addressed many of DHS's programs, operations, and activities. This report highlights our key work in these areas, but does not address all products we and the DHS IG issued related to DHS, 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.[12] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical 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.[13] 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 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 related to homeland security, and DHS's and components' strategic plans and documents. We then grouped these expectations within each functional area into broader sub-areas, as shown in appendix I. For example, we identified administering grant programs for surface transportation security as a performance expectation for DHS within the grants sub-area of the surface transportation functional area. Further, we then aligned our functional areas to the five QHSR missions based on our

[12] GAO-07-454.

[13] We focused these mission areas primarily on DHS's homeland security-related functions. We did not consider the U.S. 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.

review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents, as shown in appendix II.[14]

To identify key areas of progress and work that remains in each functional area, as well as crosscutting and management issues that have affected DHS's implementation efforts, we examined our and the DHS IG's past reports. We selected, in consultation with GAO subject matter experts, key work 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, and to supplement our work, of DHS's progress and work remaining. We identified crosscutting issues based on analysis of our work in each functional mission area to determine common issues that have affected DHS's implementation efforts across the various mission areas.

We obtained and incorporated feedback on our assessments from our subject matter experts. In addition, we provided DHS with drafts of our assessments of DHS progress and work remaining in each functional area and crosscutting issue and obtained and analyzed updated information provided by DHS on these areas. In some cases, DHS provided us with updated data on its efforts, such as statistics on technology deployments or program activities. We assessed the reliability of these data by reviewing available documentation from DHS. We determined that the data were sufficiently reliable for the purposes of our report. We included updated information in our assessments, based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment. We noted these instances in our report.

[14] Our functional areas, as well as those key sub-areas that comprise the functional areas, may pertain to more than one QHSR mission area. In cases when sub-areas within a functional area support more than one QHSR mission, we kept the sub-area with its larger functional area and noted to which other QHSR missions it aligned. We provided DHS with our alignment of the functional areas to the QHSR missions, and incorporated the department's feedback, as appropriate.

Our assessments of the progress made by DHS in functional areas and sub-areas, as well as our analyses of crosscutting issues, are based primarily on our reports, supplemented by reports of the DHS IG. As such, the assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area. Further, we do not intend to imply that our discussion of progress and work remaining in the functional areas and sub-areas, considered separately or together, reflect DHS's progress in implementing its missions. Instead, our assessments provide information on progress made and work that remains in key functional areas on which we have reported, as indicated by findings from our work, supplemented by that of the DHS IG. In addition, 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, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas. Further, for some sub-areas, we were unable to make an assessment of DHS's progress because we and the DHS IG have not conducted recent work in that area or have conducted limited work. Additionally, DHS developed other performance measures against which to gauge its progress in fiscal year 2011, but has not yet reported on these measures. As such, the department did not have data available across a consistent baseline against which to assess its progress from fiscal years 2004 through 2011. Therefore, we were not able to assess DHS's progress against a baseline for each functional area and sub-area, we did not assign a qualitative rating of progress for each area, and we did not apply a weight to the expectations or sub-areas. More detailed information on those sub-areas for which we did not make an assessment is included in appendices III through XII.

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 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. A more detailed discussion of our scope and methodology is contained in appendix II.

Background

In November 2002, the Homeland Security Act was enacted into law, creating DHS.[15] This act defined the department's missions to include preventing terrorist attacks within the United States; reducing U.S. vulnerability to terrorism; and minimizing the damages, and assisting in the recovery from, attacks that occur within the United States. The act also specified major responsibilities for the department, including to analyze information and coordinate the protection of critical infrastructure; coordinate efforts to develop countermeasures against chemical, biological, radiological, nuclear, and other emerging terrorist threats; secure U.S. borders and transportation systems; and manage the federal government's response to terrorist attacks and major disasters. Various laws have been enacted and presidential directives have been issued that, among other things, expand, modify, or clarify DHS's missions and responsibilities. For example, these laws and directives have reorganized departmental offices and functions; clarified DHS's roles and responsibilities, such as for emergency preparedness and response; and directed DHS to complete various strategic documents or implement specific programs within certain time frames. For example, the Aviation and Transportation Security Act, enacted in November 2001, established the Transportation Security Administration (TSA) and, among other things, included requirements for deploying a federal screening workforce at airports and screening all checked baggage transported on passenger aircraft using explosive detection systems.[16] The Maritime Transportation Security Act of 2002[17] and the Security and Accountability For Every Port Act of 2006 (SAFE Port Act),[18] among other things, established and modified a maritime security framework to include U.S. vessel and port facility security requirements, an international port security assessment program, and programs for scanning cargo containers. The Intelligence Reform and Terrorism Prevention Act of 2004 included provisions related to intelligence, immigration enforcement, border security, and aviation security, such as those calling for an increase in the number of Border Patrol agents and full-time investigators for violations of immigration law, subject to the availability of appropriations, and requiring DHS to develop

[15] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[16] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[17] Pub. L. No. 107-295, 116 Stat. 2064 (2002).

[18] Pub. L. No. 109-347, 120 Stat. 1884 (2006).

a national strategy for transportation security.[19] The Post-Katrina Emergency Management Reform Act of 2006 required changes to the Federal Emergency Management Agency's (FEMA) organizational and management structure, and addressed other emergency management areas, such as emergency communications, and national planning and preparedness.[20] The Implementing Recommendations of the 9/11 Commission Act of 2007 includes provisions related to critical infrastructure protection, transportation security, and chemical, biological, radiological, and nuclear threats, among other areas.[21] The law references the recommendations made by the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission).

DHS began operations in March 2003, and its establishment represented a fusion of 22 federal agencies to coordinate and centralize the leadership of many homeland security activities under a single department. The department's total budget authority has increased from about $39 billion in fiscal year 2004 to about $55 billion in fiscal year 2011.[22] The department's fiscal year 2012 budget request is about $57 billion in total funding. Table 1 provides information on DHS's budget authority for each fiscal year from 2004 though 2011, as reported by DHS.

[19] Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[20] Pub. L. No. 109-295, 120 Stat. 1394 (2006).

[21] Pub. L. No. 110-53, 121 Stat. 266 (2007).

[22] These data are not adjusted for inflation.

Table 1: DHS Budget Authority for Fiscal Years 2004 through 2011 in Thousands of Dollars, as Reported by DHS

	Fiscal year 2004	Fiscal year 2005	Fiscal year 2006	Fiscal year 2007	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010	Fiscal year 2011
U.S. Customs and Border Protection (CBP)	$5,994,287	$6,520,698	$7,970,695	$9,344,781	$10,816,001	$11,981,853	$11,846,401	$11,254,520
FEMA	$8,378,109	$74,031,032	$11,175,544	$5,223,503	$21,631,978	$10,932,016	$15,444,818	$10,462,572
U.S. Coast Guard	$7,097,405	$7,853,427	$8,782,689	$8,729,152	$9,319,760	$10,115,682	$11,150,079	$10,193,705
TSA	$4,578,043	$5,405,375	$6,167,014	$6,329,291	$6,809,359	$7,992,778	$7,656,066	$7,687,552
U.S. Immigration and Customs Enforcement (ICE)	$3,669,615	$4,244,228	$4,206,443	$4,726,641	$5,581,217	$6,054,817	$5,821,752	$5,805,420
U.S. Citizenship and Immigration Services (USCIS)	$1,549,733	$1,775,000	$1,887,850	$1,985,990	$2,902,012	$2,876,348	$2,881,597	$2,649,532
National Protection and Programs Directorate (NPPD)			$678,395	$618,577	$1,171,476	$1,188,263	$2,429,455	$2,331,197
Departmental Operations	$394,435	$527,257	$610,473	$626,123	$573,983	$859,109	$809,531	$839,291
Science and Technology Directorate (S&T)	$912,751	$1,115,450	$1,487,075	$973,109	$830,335	$932,587	$1,006,471	$827,578
Domestic Nuclear Detection Office (DNDO)				$480,968	$484,750	$514,191	$383,037	$341,744
Analysis and Operations			$252,940	$299,663	$304,500	$327,373	$333,030	$334,360
Office of Health Affairs					$118,375	$157,621	$136,850	$139,455
Office of the Inspector General	$80,318	$97,317	$84,187	$98,685	$116,711	$119,513	$134,874	$113,646

	Fiscal year 2004	Fiscal year 2005	Fiscal year 2006	Fiscal year 2007	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010	Fiscal year 2011
FEMA Office of Grant Programs[a]	$4,013,182	$3,984,846	$3,377,737	$3,393,000				
United States Visitor and Immigrant Status Indicator Technology (US-VISIT)[b]	$328,053	$340,000	$336,600	$362,494				
Border and Transportation Security Directorate[b]	$8,058	$9,617						
Information Analysis and Infrastructure Protection Directorate[b]	$834,348	$887,108						
Total	**$39,374,049**	**$108,401,920**	**$48,747,645**	**$44,946,414**	**$62,584,255**	**$56,125,581**	**$62,035,217**	**$55,006,703**

Source: GAO analysis of DHS data.

Notes: Data are rounded to the nearest thousand. The data reflect total budget authority amounts as reported to us by DHS. The amounts include annual and supplemental appropriations, rescissions, amounts reprogrammed or transferred, fee estimates, and mandatory amounts. The amounts do not reflect carryover or rescissions of unobligated balances. The FEMA fiscal year 2005 amount includes about $45 billion in supplemental funding for Hurricane Katrina.

[a] The Office of Grant Programs has undergone several realignments. It was previously known as the Office of Grants and Training in the Preparedness Directorate, the Office of State and Local Government Coordination and Preparedness, and the Office for Domestic Preparedness.

[b]The Border and Transportation Security Directorate, the Information Analysis and Infrastructure Protection Directorate, and the US-VISIT program are legacy organizations within DHS. The functions of these organizations have been realigned through DHS reorganizations. In particular, in March 2007 US-VISIT was reorganized under the National Protection and Programs Directorate. The Border and Transportation Security Directorate included U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, the Transportation Security Administration, and the Federal Law Enforcement Training Center, and had budget authority in addition to those components' amounts.

A variety of factors have affected DHS's efforts to implement its mission functions since its establishment, including several departmental reorganizations. Most notably, in 2005 DHS announced the outcome of its Second Stage Review, a systematic evaluation of DHS's operations, policies, and structures. As a result of this review, the department

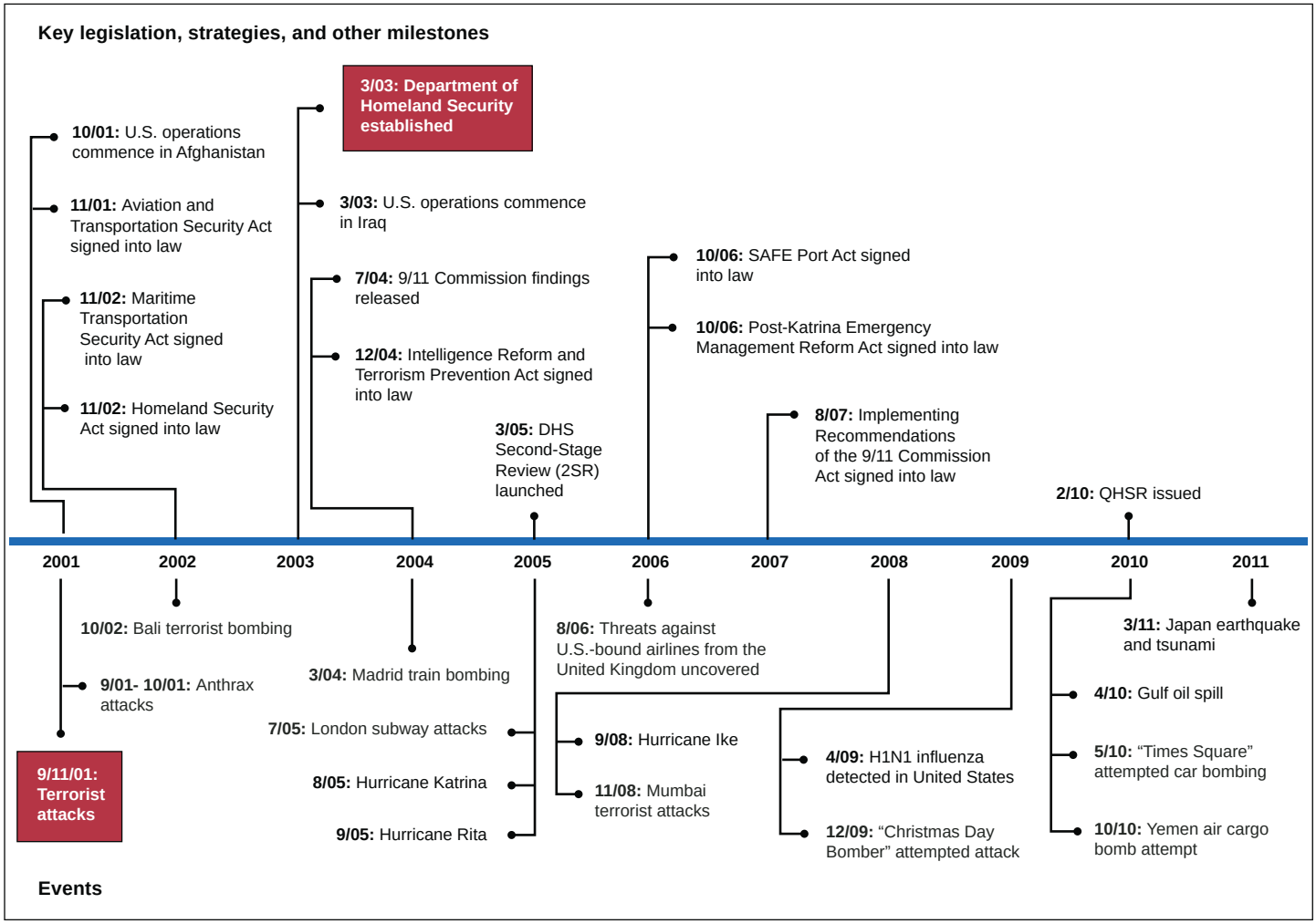
realigned existing directorates.[23] The Post-Katrina Emergency Management Reform Act provided for the further reorganization of functions within the department by, in particular, realigning DHS's emergency preparedness and response responsibilities.[24] Further, as a result of the Implementing Recommendations of the 9/11 Commission Act of 2007, DHS reorganized its intelligence-related operations.[25] In addition to these reorganizations, domestic and international events have affected DHS's implementation efforts. For example, Hurricanes Katrina and Rita, the 2009 H1N1 pandemic, the attempted airline attack on December 25, 2009, and the 2010 Gulf oil spill required rapid responses from the department and impacted DHS's plans and operations for mitigating vulnerabilities and addressing threats, and its progress in implementing its missions. Figure 1 provides a timeline of selected events that have affected DHS's implementation efforts.

[23] This reorganization realigned the Directorates for Border and Transportation Security, Information Analysis and Infrastructure Protection, and Emergency Response and Preparedness, and created the Directorates for Policy and Preparedness.

[24] Pub. L. No. 109-295, 120 Stat. 1394 (2006). Among other things, this reorganization placed certain national preparedness functions formerly in the Preparedness Directorate and legacy FEMA preparedness programs in a new National Preparedness Division within FEMA, which became responsible for policy, contingency planning, exercise coordination and evaluation, emergency management training, and hazard mitigation. In addition, the Preparedness Directorate was renamed the National Protection and Programs Directorate and retained some Preparedness Directorate elements not transferred to FEMA, such as the Office of Infrastructure Protection. Additionally, US-VISIT was moved to the new National Protection and Programs Directorate.

[25] See Pub. L. No. 110-53, 121 Stat. 266 (2007).

Figure 1: Selected Events That Have Affected DHS Implementation Efforts



Source: GAO analysis of DHS data.

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 to achieve 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.[26] 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. DHS implemented key homeland security operations and achieved 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. Specifically:

- DHS issued strategic and operational plans to guide its homeland security efforts, such as the QHSR, which provided a strategic framework for homeland security, and the *National Response Framework*, which is built upon coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector.
- DHS successfully hired, trained, and deployed workforces, such as a federal screening workforce at airports nationwide. DHS also has about 20,000 agents to patrol the U.S. land borders and about 20,600 officers to conduct screening at air, land, and sea ports of entry.
- DHS created new programs and offices, or expanded existing ones, to implement key homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to, among other things, coordinate the nation's efforts to prepare for,

[26] 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 the American population.

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, our work has shown that more work remains for DHS to address 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 canceled technology program for securing U.S. borders, known as the Secure Border Initiative Network, and some technologies for screening passengers at airport checkpoints. DHS also has not yet fully implemented its roles and responsibilities for developing and implementing key homeland security programs and initiatives. For example, FEMA 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 of 2006. [27] Further, DHS has not yet fully deployed technologies to meet key missions for border, aviation, and maritime security. Our work has also 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 program management and oversight, and better assessing homeland security requirements, needs, costs, and benefits, such as for key acquisition and technology programs.

[27] See 6 U.S.C. § 749.

Table 2 provides additional information on key progress and work remaining in each of DHS's functional mission areas, as identified by our work and supplemented by that of the DHS IG, with an emphasis on work completed since 2008. We have made approximately 1,500 recommendations to DHS to help address these issues, and DHS has addressed about half of them and has actions underway to address others. Appendixes III through XII provide more detailed information on our assessment of progress made and work remaining in each functional, including recommendations we have made and the department's efforts to implement them.

Table 2: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We Have Reported

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
Mission 1: Preventing Terrorism and Enhancing Security	Aviation security	**Key progress:** DHS has enhanced aviation security in key areas related to the aviation security workforce, passenger prescreening, passenger checkpoint screening, checked baggage security, air cargo screening, and security of airports. For example, DHS developed and implemented Secure Flight, a passenger prescreening program through which the federal government now screens all passengers on all domestic and international commercial flights to, from, and within the United States. 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 has 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 including 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.	Appendix III

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
	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.[b] 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.	Appendix IV
	Critical infrastructure protection—physical assets	**Key progress:** DHS expanded its efforts to conduct risk assessments 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 an 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.	Appendix V

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		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 take actions 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 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, among other things, 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 transportation 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.[c] Additionally, DHS's information sharing efforts would benefit from improved streamlining, coordination, and assessment of the effectiveness of information sharing mechanisms.	Appendix VI

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
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 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 improved programs designed to enhance the security of documents used to enter the United States. For example, DHS 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.	Appendix VII

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
	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, including 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.[d] 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 does 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.[e]	Appendix VIII

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
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.[f] 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 that 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.	Appendix IX
	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.	Appendix X

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		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.	
Mission 4: Safeguarding and Securing Cyberspace	Critical infrastructure protection—cyber assets	**Key progress:** DHS expanded its efforts to conduct cybersecurity risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cybersecurity 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.	Appendix XI

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: Key challenges remain in DHS's cybersecurity 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 instance, 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.	
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.	Appendix XII

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: More work remains in DHS's efforts to assess capabilities for all-hazards preparedness 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 this report.

Note: This table also includes examples from selected DHS IG reports.

[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] DHS issued three bioterrorism risk assessments in 2006, 2008, and 2010; two chemical terrorism risk assessments in 2008 and 2010; and two integrated CBRN terrorism risk assessments in 2008 and 2011. DHS also plans to issue the first radiological and nuclear terrorism risk assessment in 2011.

[c] The Implementing Recommendations of the 9/11 Commission Act of 2007 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.

[d] The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the *International Convention for the Safety of Life at Sea, 1974.* In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

[e] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

[f] 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:

- the need to integrate and strengthen its management functions;
- the need for increased utilization of performance assessments;
- the need for an enhanced use of risk information to inform planning, programming, and investment decision-making;
- limitations in effective sharing and use of terrorism-related information;
- partnerships that are not sustained or fully leveraged; and
- 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. 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.

Table 3 provides examples of crosscutting issues that have impacted the department's progress, as identified by our work. Appendixes XIII through XVIII provide more detailed information on our assessment of progress made and work remaining in each crosscutting area, including recommendations we have made and DHS's efforts to implement them.

Table 3: Crosscutting and Management Issues Affecting DHS's Progress in Implementing Its Homeland Security Missions

Crosscutting issue	Summary of key progress and work remaining	Appendix
DHS transformation and implementation	DHS has taken action to strengthen its management functions, including its acquisition, information technology, financial, and human capital management functions. DHS developed a strategy to help address these issues that includes corrective actions for mitigating its management challenges. However, DHS needs to demonstrate sustainable, measurable progress in implementing the strategy and corrective actions to address challenges we have identified within and across its management functions, as the effectiveness of these functions and their implementation affect its ability to fulfill its homeland security and other missions.	Appendix XIII
Performance measurement	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 fully 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. While improvements have been made, the department needs to continue to work to strengthen its measures to more fully assess the effectiveness and results of its programs and efforts to inform any needed adjustments.	Appendix XIV
Risk management	DHS and its component agencies developed strategies and tools for conducting risk assessments. 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.	Appendix XV
Information sharing	DHS expanded its efforts to share terrorism-related information, particularly with state and local government and private sector entities, and has initiatives underway to identify state and local partners' information needs. However, DHS could take further actions to more comprehensively identify state and local agencies' information sharing needs, establish performance measures for assessing results, and streamline its mechanisms for sharing information. Effectively sharing terrorism-related information with state and local law enforcement agencies is important, as they depend on such information to maintain situational awareness of emerging threats and to help allocate homeland security resources.	Appendix XVI
Partnerships and coordination	DHS made progress in coordinating its programs and activities with homeland security partners, but could strengthen its efforts to ensure that partners' information and other needs are met and provide enhanced oversight of coordination mechanisms. For example, with regard to border security, federal, state, local, tribal, and Canadian law enforcement partners reported improved DHS coordination to secure the northern border through mechanisms such as interagency forums that helped to establish a common understanding of border security threats. However, these partners cited ongoing challenges in sharing information and resources for daily border security related to operations and investigations.	Appendix XVII
Developing and deploying new technologies for homeland security	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.	Appendix XVIII

Source: GAO analysis based on the areas included in this report.

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

Our work on the functional mission areas and crosscutting issues discussed in this report 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, one in which a broad range of threats face the nation—from terrorists' possible use of a chemical or biological agent to carry out an attack to cyber threats and intrusions to natural disasters and infectious diseases. DHS made progress and 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. In particular, we reported that top leadership involvement and clear lines of accountability for making improvements would be critical to marshalling the needed resources and building and maintaining organizationwide commitment to new ways of doing business. 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, local, and tribal governments; the private and nonprofit sectors; and international partners. Critical aspects of DHS's success depend on well-functioning relationships with third parties, and DHS needs to continue to create and maintain a structure that can leverage partnerships to effectively implement homeland security efforts. Eight years after its establishment, DHS has made important strides in providing leadership and coordinating efforts across the enterprise as it continues to work to implement and strengthen its effectiveness across its range of missions. For example,

DHS strengthened its partnerships and collaboration with foreign governments to coordinate and standardize security practices for aviation security. It has also improved coordination and clarified roles and responsibilities with state, local, and tribal governments for emergency management. In addition, DHS operates the Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists to local communities to help foster effective information sharing with the private sector and local communities.

However, our work has found that DHS made limited progress in forging effective partnerships and sharing information throughout the enterprise early in its existence and as it matured, and although DHS continues to make improvements in this area, it faces challenges in building and leveraging these partnerships and information. These challenges have impeded the department's progress, affecting its ability to effectively and efficiently satisfy its missions. For example, we found that DHS has not effectively overseen key interagency forums its components have established with other federal, state, local, tribal, and foreign law enforcement agencies to secure the border, raising the risk of duplication, overlap, and an inefficient use of resources.

In 2005 we designated information sharing for homeland security, for which DHS has key responsibilities, 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 to protect against terrorist threats. We reported that DHS must effectively share terrorism-related information with state and local law enforcement agencies because they depend on it to maintain awareness of emerging threats and to allocate homeland security resources, among other things. Further, 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 in this area, but more work remains to strengthen and streamline existing information sharing mechanisms and better address partners' information needs. These gaps have contributed to, among other things, DHS not realizing the full potential and contributions that its partners can provide, and not maximizing its effectiveness in achieving its missions. For example, with regard to cybersecurity, private sector stakeholders reported that they expect their federal partners, including DHS, to provide usable, timely,

and actionable cyber threat information and alerts and a secure mechanism for sharing information, among other things. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations. 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 have identified the potential for overlap between various mechanisms DHS uses for sharing security-related information with public transit agencies. 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. 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.[28] However, the department has not effectively executed these processes in a number of instances, across the

[28] For example, in 2010 DHS published an acquisition management directive, which established an oversight framework to manage acquisition programs.

range of its management functions, and has not fully integrated these functions across components and among departmental missions. These issues have contributed to performance problems in programs aimed at delivering important mission capabilities. For example, DHS did not sufficiently define what capabilities and benefits would be delivered, by when, and at what cost for US-VISIT—which is to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information—and has not yet reached a decision on deploying an exit capability. Not defining these capabilities and benefits contributed to development and deployment delays. In another example, 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 this program.

In 2003, GAO designated the transformation and implementation of DHS as high risk because the department 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. Eight years later, DHS remains on our high-risk list. DHS has made important strides in working to strengthen its management functions, has established plans to strengthen and integrate these functions, and in recent years has demonstrated strong leadership support to address these long-standing issues. In particular, 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, more work remains to position these management areas for success. For example, DHS does not yet have enough skilled personnel to carry out activities in some key programmatic and management areas, such as for acquisition management, and was ranked 28 out of 32 agencies in the 2010 Partnership for Public Service's Best Places to Work in the Federal

Government rankings.[29] DHS also has not yet implemented an integrated financial management system, impeding its ability to have ready access to information to inform decision-making, and has been unable to obtain a clean audit opinion on the audit of its consolidated financial statements since its establishment. Moving forward, addressing these management challenges will be critical for DHS's success, as will 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 initiatives, and responding to adapting adversaries and evolving threats was and is a significant challenge facing DHS. Key threats and incidents that have emerged, both domestically and internationally, such as the anthrax attacks, Hurricanes Katrina and Rita, and a number of attempted attacks against the aviation sector, have impacted and altered the department's approaches and investments. For example, DHS made key changes to its processes and technology investments for screening passengers and baggage at airports in part as a result of threats facing commercial aviation. DHS also changed its processes and clarified roles and responsibilities for emergency management in the aftermath of Hurricanes Katrina and Rita.

It is understandable that these events and threats had to be addressed as they arose. However, our work has shown, throughout the department, that limited strategic and program planning, as well as assessment and evaluation to inform approaches and investment decisions, have contributed to programs not meeting strategic needs or doing so effectively and efficiently. 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

[29] Partnership for Public Service and the Institute for the Study of Public Policy Implementation at the American University School of Public Affairs, *The Best Places to Work in the Federal Government* (Washington, D.C.: 2010).

capabilities, as required by the Post-Katrina Emergency Management Reform Act of 2006 and Presidential Policy Directive 8: National Preparedness, it cannot effectively evaluate and identify key capability gaps and target limited resources to fill those gaps. We have also reported that while DHS has made important progress in assessing and analyzing risk across sectors, 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, the 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. Enhanced assessment of programs' performance and the use of that information to inform decisions will provide the department with important insights in determining the extent to which programs and operations are meeting intended goals and results and at what cost.

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 of feasible alternatives; and, as appropriate, adjustment of programs or operations that are not meeting mission needs. For example, TSA'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, TSA 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. Further, with regard to border security efforts, CBP established performance measures for its checkpoints to indicate checkpoint contributions toward apprehending removable aliens and seizing illegal drugs, but the lack of information on those passing through checkpoints undetected continued to challenge CBP's ability to measure checkpoint effectiveness and provide public accountability. 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, that these programs are sustainable, and that they 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. Specifically, DHS has taken many actions to (1) develop strategic and operational plans across its range of missions; (2) hire, deploy and train workforces; (3) establish new, or expand existing, offices and programs; and (4) develop and issue policies, procedures, and regulations to govern its homeland security operations. 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. We have made about 1,500 recommendations to DHS to address these issues, which the department has or is working to implement, but more work remains. 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.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for its review and comment. We received written comments on the draft report from DHS, which are reproduced in full in appendix XIX. DHS also provided technical comments, which we incorporated as appropriate.

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. For example, the department noted its creation and management of the Visa Security Program, which is operational at 19 posts in 15 countries; the increase in the number of deployed Border Patrol agents since 2001; the establishment of fusion centers to serve as focal points for the analysis and sharing of threat and vulnerability-related information; passenger screening and prescreening efforts; and support to state, local, tribal and territorial partners' efforts to enhance emergency communications capabilities, among other things. DHS further noted its issuance of the Quadrennial Homeland Security Review in February 2010, which outlined a strategic framework for homeland security. We recognize the department's progress in these and other areas in the report, as well as discuss existing challenges that will be important for DHS to address moving forward.

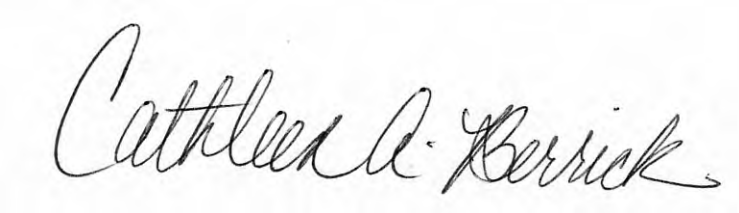
The department also stated that the report does not address all of DHS's homeland security-related activities and efforts, and that assessments in each area are not comprehensive because we and the DHS IG have

completed varying levels of work in each area. The report notes that the results are based on our work on DHS since it began operations, supplemented with work completed by the DHS IG, with an emphasis on work completed since 2008. We also examined updated information and documentation provided by the department in July and August 2011. As identified in the report, we highlighted our work on key DHS programs and efforts, but neither addressed all products that we and the DHS IG issued related to DHS, nor addressed all of DHS's homeland security-related activities and efforts. In addition, each mission area appendix provides examples of other DHS programs and efforts on which we and the DHS IG have not reported or have completed limited work. Thus, this report was not intended to cover all of DHS's homeland security-related activities and efforts. Further, as discussed in the report, 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, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas.

In addition, DHS provided examples of activities and programs that it stated are not reflected in our report that demonstrate progress DHS made in preparing the nation to respond to threats. These programs include the Western Hemisphere Travel Initiative and increased coordination across the federal government to analyze travel-related data, such as through watchlist centers that provide information regarding potential terrorist travel—the Federal Bureau of Investigation's Terrorist Screening Center, the National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center. This report discusses progress made and work remaining related to the Western Hemisphere Travel Initiative within the border security area. With regard to the various centers, this report acknowledges the activities of the National Targeting Center, but we did not include it in our assessments of progress because we and the DHS IG have completed limited work on it. The other three centers identified by DHS are not managed by the department. Because this report is focused on DHS-specific programs and efforts on which we have previously reported, supplemented by the work of the DHS IG, this report does not discuss these centers.

This report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-3404, or berrickc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors are listed in appendix XX.



Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues

Appendix I: Department of Homeland Security Functional Mission Areas, Sub-Areas, and Performance Expectations

Table 4 presents the performance expectations and sub-areas we identified for each Department of Homeland Security (DHS) functional mission area.

Table 4: DHS Functional Areas, Sub-Areas, and Performance Expectations

Functional Mission Area: Aviation Security
Sub Area #1: Security Workforce
1a: Ensure the screening of airport workers against terrorist watchlist records
1b: Hire and deploy a federal screening workforce
1c: Develop standards for determining aviation security staffing at airports
1d: Establish standards for training and testing the performance of airport screener staff
1e: Establish a program and requirements to allow eligible airports to use a private screening workforce
1f: Train and deploy federal air marshals on high-risk flights
1g: Establish standards for training flight and cabin crews
1h: Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts
1i: Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action
Sub Area #2: Passenger Prescreening
2a: Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List[a]
2b: Develop and implement an international passenger prescreening process to compare passenger information to terrorist watchlists before aircraft departure
Sub Area #3: Checkpoint Screening
3a: Develop and implement processes and procedures for physically screening passengers at airport checkpoints
3b: Develop and test checkpoint technologies to address vulnerabilities
3c: Deploy checkpoint technologies to address vulnerabilities
3d: Establish a program for armed law enforcement officers traveling by commercial aircraft
3e. Utilize behavioral and appearance indicators to identify persons who pose a risk to aviation security
Sub Area #4: Checked Baggage Screening
4a: Deploy explosive detection systems and explosive trace detection systems to screen checked baggage for explosives
4b: Develop a plan to deploy in-line and other optimal baggage screening systems at airports, as appropriate
4c: Pursue the deployment and use of in-line or other optimal baggage screening systems at airports, as appropriate
Sub Area #5: Air Cargo Security
5a: Develop a plan for air cargo security
5b: Develop and implement procedures to screen domestic and in-bound international air cargo
5c: Develop and implement technologies to screen air cargo

Sub Area #6: Security of Airports
6a: Establish standards and procedures for effective airport perimeter security
6b: Establish standards and procedures to effectively control access to secured airport areas
6c: Establish procedures for implementing biometric identifier systems for secured airport areas access control
Sub Area #7: Aviation Security Strategic Planning and Coordination
7a: Develop and implement a strategic and risk-based approach for aviation security functions
7b: Strengthen aviation security through partnerships, coordination and information sharing
Functional Mission Area: Chemical, Biological, Radiological, and Nuclear Threats
Sub Area #1: Assessment
1a: Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities
Sub Area #2: Detection and Mitigation
2a: Coordinate deployment of chemical, biological, radiological, and nuclear detection and other mitigation capabilities
2b: Assess and evaluate chemical, biological, radiological, and nuclear detection capabilities and other countermeasures
Functional Mission Area: Critical Infrastructure Protection—Physical Assets
Sub Area #1: Risk Assessment and Planning
1a: Develop a comprehensive national plan for critical infrastructure protection
1b: Establish and maintain a national database of critical systems and assets
1c: Identify and assess risks to critical infrastructure
Sub Area #2: Protection and Resiliency
2a: Provide and coordinate incident response and recovery planning efforts for critical infrastructure
2b: Support efforts to reduce risks to critical infrastructure
Sub Area #3 Partnerships and Coordination Mechanisms
3a: Improve and enhance public/private information sharing involving attacks and risks
3b: Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector
3c: Develop and enhance national analysis and warning capabilities for critical infrastructure
Functional Mission Area: Surface Transportation Security
Sub Area #1: Risk Assessment and Planning
1a: Develop and adopt a strategic approach for implementing surface transportation security functions
1b: Conduct threat, criticality, and vulnerability assessments of surface transportation assets
Sub Area #2: Standards, Inspections, and Training
2a: Issue standards for securing surface transportation modes
2b: Conduct inspections of surface transportation systems
2c: Develop programs to detect contraband and undeclared passengers entering the United States by rail and for tracking the shipment of security-sensitive materials
2d: Provide surface transportation security training
2e: Train and deploy explosives detection canine teams

Sub Area #3: Grants
3a: Administer grant programs for surface transportation security
Sub Area #4: Information Sharing
4a: Share information with stakeholders to enhance surface transportation security
Functional Mission Area: Border Security
Sub Area #1: Inspection of Individuals at Ports of Entry
1a: Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry
1b: Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry
Sub Area #2: Inspection of Cargo and Goods at Ports of Entry while Facilitating Commerce
2a: Develop and implement strategies to detect and interdict illegal flows of cargo, drugs, and other items into and out of the United States while facilitating legitimate commerce
Sub Area #3: Securing the Border between Ports of Entry
3a: Develop and implement programs to detect and identify illegal border crossings between ports of entry
3b: Leverage technology, infrastructure, personnel, and information to secure the border between ports of entry
Sub Area #4: Enhancing Security in the Visa Issuance and Travel Documentation Process
4a: Enhance security measures in the visa issuance process
4b: Enhance the security of certain documents used to enter the United States
Sub Area #5: Collaborating on Border Security Efforts
5a: Enhance collaboration with international, federal, state, local, and tribal law enforcement as well as community groups and the private sector to increase border security, exchange relevant information, and facilitate commerce
Sub Area #6: Border Security Resources
6a: Ensure adequate assets and facilities (at ports of entry for moving people and cargo)
6b: Provide adequate training and equipment for all border-related employees
6c: Develop and implement staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission
Functional Mission Area: Maritime Security
Sub Area #1: Port Facility and Vessel Security
1a: Develop regional (port-specific) plans for security
1b: Develop regional (port-specific) plans for response
1c: Develop regional (port-specific) plans for recovery
1d: Develop, update, and coordinate protocols for resuming trade after a transportation security disruption or incident
1e: Ensure port facilities have completed vulnerability assessments and developed and implemented security plans
1f: Implement a port security grant program to help facilities improve their security capabilities
1g: Implement a national facility access control system for port secured areas
1h: Ensure that vessels have completed vulnerability assessments and developed and implemented security plans
1i: Exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts

Sub Area #2: Maritime Domain Awareness and Information Sharing
2a: Develop a national plan to establish and improve maritime intelligence
2b: Establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level
2c: Collect and analyze information on incoming vessels to assess risks and threats
2d: Develop and implement a vessel-tracking system to improve intelligence and maritime domain awareness on vessels in U.S. waters
2e: Develop and implement a long-range vessel tracking system to improve maritime domain awareness
2f: Identify and address homeland security needs in the Arctic
2g: Develop and implement an international port security program to assess security at foreign ports
Sub Area #3: International Supply Chain Security
3a: Collect and analyze information on arriving cargo for screening purposes
3b: Develop and implement a system for screening and inspecting cargo for illegal contraband and radiation
3c: Develop and implement a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports
3d: Develop and implement a program to work with the private sector to improve and validate supply chain security
3e: Develop standards for cargo containers to ensure their physical security
Sub Area #4: National Planning
4a: Develop national plans for maritime security
4b: Develop national plans for maritime response
4c: Develop national plans for maritime recovery
Functional Mission Area: Immigration Enforcement
Sub Area #1: Investigations of Immigration Offenses
1a: Develop and implement strategies and programs to enforce immigration laws at the workplace
1b: Develop and implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States
1c: Develop and implement a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity
Sub Area #2: Investigations of Customs Offenses
2a: Disrupt and dismantle cross-border mechanisms for money laundering and financial crimes
2b: Investigate illegal imports and exports that threaten public safety, including illicit commodities, weapons, and drugs
Sub Area #3: Identification, Detention, and Removal of Aliens Subject to Removal
3a: Develop and implement programs to ensure the timely identification, prioritization, and removal of noncriminal aliens subject to removal from the United States
3b: Develop and implement a program to screen and respond to local law enforcement and community reports of aliens who may be subject to removal from the United States
3c: Ensure the identification, prioritization, and removal of criminal aliens subject to removal from the United States
3d: Assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal
3e: Develop and implement a program to allow for the secure alternative detention of noncriminal aliens subject to removal

Sub Area #4: Management and Training of Immigration Enforcement Human Capital
4a: Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's immigration enforcement mission
4b: Provide training, including foreign language training, and equipment for all immigration enforcement personnel to fulfill the agency's mission
Functional Mission Area: Immigration Services
Sub Area #1: Administration of Immigration Benefits
1a: Institute process and staffing reforms to improve application processes
1b: Eliminate the benefit application backlog and reduce application completion times to 6 months
1c: Implement programs to prevent future backlogs from developing
1d: Establish revised immigration application fees based on a comprehensive fee study
1e: Capture biometric information on all benefits applicants
1f: Implement an automated background check system to track and store all requests for immigration benefits
1g: Establish online access to status information about benefit applications
1h: Establish online filing for benefit applications
1i: Communicate immigration-related information to other relevant agencies
1j: Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications
1k: Institute a case management system to manage applications and provide management information
Sub Area #2: Immigration Benefit Fraud
2a: Create and maintain an office to reduce immigration benefit fraud
2b: Establish and enhance training programs to reduce fraud in the benefits process
2c: Implement a fraud assessment program to reduce benefit fraud
Sub Area #3: Immigrant Integration
3a: Promote immigrant integration by enhancing understanding of U.S. citizenship and providing support to immigrants through the naturalization process
Functional Mission Area: Critical Infrastructure Protection—Cyber Assets
Sub Area #1: Risk Assessment and Planning
1a: Develop a comprehensive national plan for critical infrastructure protection
1b: Establish and maintain a national database of critical systems and assets
1c: Identify and assess risks to critical infrastructure
Sub Area #2: Protection and Resiliency
2a: Provide and coordinate incident response and recovery planning efforts for critical infrastructure
2b: Support efforts to reduce risks to critical infrastructure
Sub Area #3: Partnerships and Coordination Mechanisms
3a: Improve and enhance public/private information sharing involving attacks and risks
3b: Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector
3c: Develop and enhance national analysis and warning capabilities for critical infrastructure

Functional Mission Area: Emergency Preparedness and Response
Sub Area #1: National Emergency Preparedness and Response Planning
1a: Develop a national incident management system
1b: Coordinate implementation of a national incident management system
1c: Establish and implement an all-hazards national response framework
1d: Coordinate implementation of an all-hazards response framework
1e: Develop a complete inventory of federal response capabilities
1f: Develop a national, all-hazards preparedness goal
1g: Develop a national preparedness system
1h: Develop a national preparedness report
1i: Support citizen participation in national preparedness efforts
1j: Develop plans and capabilities to strengthen nationwide recovery efforts
1k: Conduct and support risk assessments and risk management capabilities for emergency preparedness
1l: Establish a comprehensive preparedness assessment system
Sub Area #2: Provision of Emergency Assistance and Services
2a: Develop the capacity to provide needed emergency assistance and services in a timely manner
2b: Provide timely assistance and services to individuals and communities in response to emergency events
2c: Provide oversight of emergency response contracts
Sub Area #3: Emergency and Interoperable Communications
3a: Implement a program to improve interoperable communications among federal, state, and local agencies
3b: Implement procedures and capabilities for effective interoperable communications
3c: Increase the development and adoption of interoperability communications standards
3d: Develop and implement performance goals and measures to assess progress in developing interoperability
3e: Provide grant funding to first responders in developing and implementing interoperable communications capabilities
3f: Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities
3g: Coordinate research, development, and testing efforts to identify and develop technologies to facilitate sharing of emergency alerts and threat-related information
Sub Area #4: Support to State and Local Partners
4a: Provide assistance to state and local governments to develop all-hazards plans and capabilities
4b: Administer a program for providing grants and assistance to state and local governments and first responders
4c: Allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors
Sub Area #5: Emergency Preparedness Best Practices and Training and Exercise Programs
5a: Develop a system for collecting and disseminating lessons learned, best practices, and threat information to emergency responders and other relevant stakeholders
5b: Establish a comprehensive training program for national preparedness
5c: Establish a program for conducting emergency preparedness exercises

Sub Area #6: Emergency Preparedness Human Capital Management
6a: Develop and implement a strategic human capital plan, including filling vacancies and standards for credentialing personnel
6b: Ensure the capacity and readiness of disaster response teams

Source: GAO analysis.

[a] The Selectee and No-Fly lists contain the names of individuals with known or appropriately suspected links to terrorism. These lists are subsets of the federal government's consolidated terrorist watchlist that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

Appendix II: Scope and Methodology

This report addresses the following question: What progress has the Department of Homeland Security (DHS) made in implementing its mission functions since it began operations; what work, if any, remains; and what crosscutting and management issues have affected DHS's implementation efforts?

This report is based primarily on work that we have completed since DHS began its operations in March 2003, with an emphasis on reports issued since 2008 to reflect our most recent work, supplemented by DHS Office of Inspector General (IG) reports and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on key DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, we examined program documentation and interviewed agency officials, among other things.

To determine what progress DHS has made in implementing its mission functions and what work, if any, remains, we identified 10 DHS functional areas within its missions, 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 Quadrennial Homeland Security Review (QHSR) and budget documents, such as its congressional budget justifications.[1] We discussed these functional areas with our subject matter experts and DHS officials and incorporated their feedback as appropriate.[2] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical 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

[1] GAO-07-454.

[2] Our subject matter experts are individuals within GAO who have directed or managed work related to the DHS functional areas.

response.[3] 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 requirements, responsibilities, and goals set for the department by Congress, the administration, and DHS 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:

- Homeland security-related laws enacted since September 2006 to identify legislative requirements for each DHS functional area.[4] Examples of such laws include the Implementing Recommendations of the 9/11 Commission Act of 2007,[5] the Security and Accountability For Every Port Act of 2006 (SAFE Port Act),[6] and the Post-Katrina Emergency Management Reform Act of 2006.[7]
- DHS appropriation acts and accompanying conference reports for fiscal years 2006 through 2011 to identify requirements established and guidance provided to DHS for each functional area.
- Presidential directives and executive orders that have been issued since September 2006 to identify expectations set for DHS by the administration for each functional area. Examples of such directives include Homeland Security Presidential Directive 25: Arctic Region Policy, and Presidential Policy Directive 8: National Preparedness.

[3] We focused these mission areas primarily on DHS's homeland security-related functions. We included U.S. Citizenship and Immigration Services' activities for administering immigration benefits in this report, as they are related to homeland security issues, such as detecting immigration benefit fraud, and are included in the Quadrennial Homeland Security Review. 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 we 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.

[4] We analyzed homeland security-related laws enacted since September 2006 because we had analyzed homeland security-related laws enacted through September 2006 when identifying the expectations we reported in our August 2007 report.

[5] Pub. L. No. 110-53, 121 Stat 266 (2007).

[6] Pub. L. No. 109-347, 120 Stat. 1884 (2006).

[7] Pub. L. No. 109-295, 120 Stat. 1394 (2006).

- Homeland security-related national strategies that have been issued since September 2006 to identify expectations set for DHS by the administration for each functional area. Examples of such strategies include the 2010 National Security Strategy and 2007 National Strategy for Homeland Security.
- Strategic plans and documents that have been issued since September 2006 by DHS and its component agencies to identify goals and measures established by the department for each functional area. Examples of such strategic plans and documents include the QHSR and Bottom-Up Review (BUR) reports, as well as component level strategic plans, such as the *U.S. Immigration and Customs Enforcement (ICE) Strategic Plan (Fiscal Year 2010-2014)*.

We then grouped the expectations we identified within each functional area into broader sub-areas. Table 5 provides an example of performance expectations and sub-areas for the border security functional area. Appendix I provides the complete list of functional areas, sub-areas, and performance expectations.

Table 5: Example of Performance Expectations and Sub-Areas for Border Security

Functional area	Sub-areas	Performance expectations
Border security	Inspection of individuals at ports of entry	Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry
		Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry
	Inspection of cargo and goods at ports of entry while facilitating commerce	Develop and implement strategies to detect and interdict illegal flows of cargo, drugs, and other items into and out of the United States while facilitating legitimate commerce
	Securing the border between ports of entry	Develop and implement programs to detect and identify illegal border crossings between ports of entry
		Leverage technology, infrastructure, personnel, and information to secure the border between ports of entry
	Border security resources (facilities, assets, and human capital)	Ensure adequate assets and facilities (at ports of entry for moving people and cargo)
		Provide adequate training and equipment for all border-related employees
		Develop and implement staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission
	Enhancing security in the visa issuance and travel documentation processes	Enhance security measures in the visa issuance process
		Enhance the security of certain documents used to enter the United States

Functional area	Sub-areas	Performance expectations
	Collaborating border security efforts	Enhance collaboration with international, federal, state, local, and tribal law enforcement as well as community groups and the private sector to increase border security, exchange relevant information, and facilitate commerce

Source: GAO analysis.

To identify the performance expectations and sub-areas, one analyst independently reviewed the source documents to identify expectations and sub-areas for a functional area. A second analyst then independently reviewed and verified each analysis. We also obtained and incorporated feedback from our subject matter experts on the expectations and sub-areas. In addition, we obtained feedback from DHS and component officials on the expectations and sub-areas we identified, and incorporated their feedback as appropriate.

Further, we then aligned our functional areas to the five Quadrennial Homeland Security Review (QHSR) missions based on our review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents (see table 6). Within these documents, DHS identified how its initiatives, programs, and activities align or support each QHSR mission, with some supporting more than one mission. For example, U.S. Customs and Border Protection (CBP) identified that its efforts related to inspections at ports of entry and facilitation of trade primarily support QHSR Mission 2: Securing and Managing Our Borders, but also, to a lesser extent, support QHSR Mission 1: Preventing Terrorism and Enhancing Security and Mission 3: Enforcing and Administering Our Immigration Laws. On the basis of DHS's alignment of its initiatives, programs, and activities to QHSR missions, we grouped the 10 functional areas under DHS's QHSR missions. In doing so, we recognized that our functional areas, as well as those key sub-areas that comprise the functional areas, may pertain to more than one QHSR mission area. For example, under our functional area of immigration enforcement, our work addressing the sub-area investigations of immigration offenses addresses DHS programs and activities that relate to more than one QHSR mission—primarily Mission 3: Enforcing and Administering Our Immigration Laws, and also Mission 2: Securing and Managing Our Borders and Mission 1: Preventing Terrorism and Enhancing Security. In those cases when a functional area aligned to more than one QHSR mission, we categorized it under the QHSR mission that it primarily supported on the basis of our review of DHS's QHSR and budget-related documents. In cases when sub-areas within a functional area supported more than one QHSR mission, we kept the sub-area with its functional area (e.g., aviation security) and noted to

which other QHSR missions it aligned. We provided DHS with our alignment of the functional areas to the QHSR missions, and incorporated the department's feedback, as appropriate.

Table 6: Alignment of Functional Areas under DHS's QHSR Missions

QHSR mission	Functional areas and sub-areas
Mission 1: Preventing Terrorism and Enhancing Security	**Aviation security** • Security of airports • Aviation security workforce • Passenger prescreening • Checkpoint screening • Checked baggage screening • Air cargo security • Aviation security strategic planning and coordination **Chemical, biological, radiological, and nuclear threats** • Assessment • Detection and mitigation **Critical infrastructure protection—physical assets** • Risk assessment and planning • Protection and resiliency • Partnerships and coordination mechanisms **Surface transportation security** • Risk assessment and planning • Security standards, inspections, and training • Grants • Information sharing
Mission 2: Securing and Managing Our Borders	**Border security** • Inspection of individuals at ports of entry • Inspection of cargo and goods at ports of entry while facilitating commerce • Securing the border between land ports of entry • Border security resources • Enhancing security in the visa issuance and travel documentation process • Collaborating on border security efforts • Border security resources **Maritime security** • Port facility and vessel security • Maritime domain awareness and information sharing • International supply chain security • Maritime security national planning

QHSR mission	Functional areas and sub-areas
Mission 3: Enforcing and Administering Our Immigration Laws	**Immigration enforcement** • Investigations of immigration offenses • Investigations of customs offenses • Identification, detention, and removal of aliens subject to removal • Management and training of immigration enforcement human capital **Immigration services** • Administration of immigration benefits • Immigration benefit fraud • Immigrant integration
Mission 4: Safeguarding and Securing Cyberspace	**Critical infrastructure protection—cyber assets** • Risk assessment and planning • Protection and resiliency • Partnerships and coordination mechanisms
Mission 5: Ensuring Resilience to Disasters	**Emergency preparedness and response** • National emergency preparedness and response planning • Provision of emergency assistance and services • Emergency and interoperable communications • Support to state and local partners • Emergency preparedness and response best practices and training and exercises programs • Emergency preparedness and response human capital management

Source: GAO analysis of DHS information.

To identify key areas of progress and work that remains in the DHS functional areas, we examined our and the DHS IG's past reports on DHS missions, programs, and operations, including recommendations we and the DHS IG have made, and actions DHS has taken or has underway to address them. We also identified preliminary observations from our ongoing work in some key areas. In doing so, we identified factors that have affected DHS progress in the functional areas. Our work and the work of the DHS IG have covered many of DHS's key programs, operations, and activities. In this report, we highlight our key work in these areas, but do not address all products we or the DHS IG have issued related to DHS, nor did we address all of the sub-areas or DHS's homeland security-related activities and efforts. We selected, in consultation with our subject matter experts, key work we and the DHS IG have completed related to the functional areas and sub-areas. 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, and to supplement our work,

of DHS's progress and work remaining. In addition, we obtained data from DHS on its budget authority for fiscal years 2004 through 2011, and funding and staffing levels related to the functional areas, and assessed the reliability of that data by available documentation. We determined that the data were sufficiently reliable for the purposes of our report.

We obtained and incorporated feedback on our assessments within the sub-areas and functional areas from our subject matter experts. In addition, we provided DHS with drafts of our assessments of DHS progress and work remaining in each functional area and obtained and analyzed updated information provided by DHS on these areas. In some cases, DHS provided us with updated data on its efforts, such as statistics on technology deployments or program activities. We assessed the reliability of these data by reviewing available documentation from DHS. We determined that the data were sufficiently reliable for the purposes of our report. We included updated information in our assessments of each sub-area and functional area, based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment, or DHS's reported actions were in the early stages of implementation, and thus it was too early to assess the results of these efforts. We noted these instances in our report.

To identify crosscutting and management issues that have affected DHS's implementation efforts, we analyzed the assessments of progress and work that remains in each functional area. We also examined our and the DHS IG's past reports on crosscutting issues, related recommendations, and actions taken by DHS or that are underway to address the recommendations. We obtained and incorporated feedback on the crosscutting issues we identified from our subject matter experts. In addition, we obtained and incorporated feedback from DHS on our assessment of crosscutting issues that have affected the department's mission implementation efforts, including updated information from DHS pertaining to these crosscutting issues. We incorporated updated information into our assessments based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment. We noted these instances in our report.

Our assessments of the progress made by DHS in the functional areas and sub-areas, as well as our analyses of crosscutting issues, are based

primarily on our issued reports, and supplemented by DHS IG reports. As such, the assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area. Additionally, we do not intend to imply that our discussion of progress and work remaining in the functional areas and sub-areas, considered separately or together, reflect DHS's progress in implementing all of its missions. We also did not assign a qualitative rating of progress for each area. DHS developed other performance measures against which to gauge its progress in fiscal year 2011, but has not yet reported on these measures. As such, the department did not have data available across a consistent baseline against which to assess its progress from fiscal years 2004 through 2011. Therefore, we were not able to assess DHS's progress against a baseline for each functional area and sub-area, and we did not apply a weight to the expectations or sub-areas. We also did not consider DHS component agencies' funding levels or the extent to which funding levels have affected the department's ability to carry out its missions as this was not included in the scope of our prior reviews. Further, we did not consider the extent to which competing priorities; external and internal events, such as departmental reorganizations; and resource demands have affected DHS's progress in each area relative to other areas, although competing priorities, events, and resource demands have affected DHS's progress in specific areas.

In addition, 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, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas. Further, for some sub-areas, we were unable to make an assessment of DHS's progress because we and the DHS IG have not conducted recent work in that area or have conducted limited work. More detailed information on those sub-areas for which we did not make an assessment is included in appendices III through XII.

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 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.

Appendix III: Aviation Security

What This Area Includes

Source: TSA.

TSA Employee Demonstrating Use of Advanced Imaging Technology.

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the lead federal agency responsible for securing all modes of transportation, including aviation. As part of these responsibilities, TSA performs or oversees the performance of security operations at the nation's more than 460 commercial airports.[1] Key elements that comprise aviation security include:

- the aviation security workforce, including hiring, training, and deploying a screening workforce;
- passenger prescreening—comparing passenger information to the Selectee and No Fly lists;[2]
- passenger checkpoint screening, including using staff, policies and procedures, and technology to address potential vulnerabilities;
- checked baggage screening, including deploying explosives detection systems and other technologies to screen baggage for explosives;
- air cargo screening, which involves using staff, policies and procedures, and technology to screen domestic and high-risk international inbound air cargo transported on passenger aircraft; and
- security of airports, including airport perimeter security and access controls.

For fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion.[3] Aviation security falls primarily within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to aviation security also include aviation security

[1] For purposes of this report, the term "commercial airport" refers to a U.S. airport operating under a TSA-approved security program and subject to TSA regulation and oversight. See 49 C.F.R. pt. 1542.

[2] The Selectee and No Fly lists contain the names of individuals with known or appropriately suspected links to terrorism. These lists are subsets of the federal government's consolidated terrorist watchlist that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

[3] In addition to TSA, DHS's U.S. Customs and Border Protection plays a role in aviation security by reviewing the passenger and crew manifest of all air carriers destined to the United States.

strategic planning and coordination, we are not reporting on this area. TSA also relies upon additional programs to deter, detect, and disrupt persons or threats posing a potential risk to aviation security, such as travel document checkers, who examine tickets and forms of identification; random employee screening; intelligence gathering and analysis; random canine team searches at airports; federal air marshals, who provide federal law enforcement presence on selected flights; and reinforced cockpit doors; as well as other measures both visible and invisible to the public. Further, TSA has additional plans and programs related to aviation security, such as TSA's plans to conduct a pilot program on expedited checkpoint screening for low-risk travelers, and TSA's Transportation Systems Integration Facility which supports the development and deployment of new technologies. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that over the past 10 years, TSA has enhanced aviation security in key areas related to the aviation security workforce, passenger prescreening, passenger checkpoint screening, checked baggage screening, air cargo security, and security of airports. For example, TSA hired, trained, and deployed a federal screening workforce. Additionally, after initial difficulty in fielding the program, TSA developed and implemented Secure Flight, a passenger prescreening program through which the federal government now screens all passengers on all domestic and international commercial flights to, from, and within the United States. DHS also developed new programs and is utilizing new technologies to screen passengers and checked baggage, and enhanced the security of domestic and in-bound air cargo. TSA also strengthened security at U.S. airports by assessing risks to airport perimeters and access controls. However, our work has shown that more work remains in these areas. For example, a risk-based strategy and a cost-benefit analysis of airport checkpoint technologies would improve passenger checkpoint screening. Further, TSA does not yet have a procurement plan and schedule for checked baggage screening technologies that would better position TSA to meet recently enhanced explosive detection requirements. Additionally, TSA does not yet have a mechanism to verify the accuracy of domestic and inbound air cargo screening data. Finally, the security of airports would be strengthened by establishing an evaluation plan for pilot tests to screen workers. Table 7 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 7: Assessment of Progress and Work Remaining in Key Aviation Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Aviation security workforce	TSA hired, trained, and deployed a federal screening workforce and other personnel, and deployed programs to enhance in-flight security.	**TSA maintains a federal screening workforce and has deployed programs for in-flight security.** **Key progress:** TSA continues to hire, train, and deploy a federal aviation security workforce. For example, TSA successfully hired, trained, and deployed a federal screening workforce to assume security screening responsibilities at commercial airports nationwide, and developed standards for determining transportation security officer staffing levels at airports. These standards formed the basis of TSA's Staffing Allocation Model, which the agency uses to determine screener staffing levels at airports. In December 2007, we reported that TSA developed a plan that identified the process the agency planned to use to review and validate the staffing model's assumptions on a periodic basis. In July 2011, TSA reported that it was conducting studies on how the staffing model might be adjusted for airport specific environmental factors (e.g., time needed for officers to get to and from off-site training facilities). In addition, TSA has deployed programs and personnel to enhance in-flight security, including training and deploying federal air marshals on high-risk flights, establishing standards for training flight and cabin crews, and establishing a Federal Flight Deck Officer program to select, train, and allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts.
		TSA established explosives detection and other training programs for its screener workforce. **Key progress:** TSA established and continues to deploy numerous programs to train and test the performance of its screening workforce. Among other efforts, TSA provided enhanced explosives-detection training, and reported developing a monthly recurrent (ongoing) training plan for all transportation security officers. In October 2010, the DHS IG reported that, with respect to transportation security officers, the agency lacked standard processes to assign on-the-job training responsibilities. The DHS IG also reported that the agency lacked standard processes to use officer test results to evaluate training program results and evaluate workforce and training needs. The DHS IG recommended that TSA finalize the documentation and implementation of a comprehensive methodology for its transportation security officer training program, and establish and document an on-the-job training program with specific criteria for transportation security officers to serve as on-the-job monitors. TSA concurred with this recommendation and took steps to address it by, for example, updating the draft version of its curriculum development reference guide. In July 2011, TSA reported that it plans to initiate studies to assess the allocation of computers and tools for training.

Area	Overall assessment	Summary of key progress and work remaining
Passenger prescreening	TSA developed and implemented Secure Flight, a government-operated system that prescreens all passengers traveling to, from, or within the United States.	**TSA prescreens all passengers traveling to, from, or within the United States through its Secure Flight program.** **Key progress:** Passenger prescreening is the matching of airline passenger information against terrorist watchlist records. To conduct this watchlist matching, TSA developed and implemented Secure Flight, a government-operated system that prescreens all passengers traveling to, from, or within the United States. In April 2010, we reported that after initial problems in fielding the program, TSA generally achieved all of the 10 statutory conditions related to the development of the Secure Flight program. The statutory conditions addressed issues such as establishing a process for passengers to correct erroneous information; operational safeguards to reduce opportunities for abuse; and appropriate life-cycle cost estimates.[a] As of June 2010, TSA deployed Secure Flight to cover all domestic and international flights operated by U.S. air carriers, and as of November 2010, to foreign air carriers with commercial flights into, out of, and within the United States.[b] In July 2011, TSA estimated that, on average, Secure Flight prescreens 2 million passenger enplanements per day.[c] TSA also estimated that, on average, Secure Flight identifies more than 200 matches against the No Fly and Selectee lists per month.[d] TSA also reported that it is in the process of implementing Secure Flight reporting for covered flights that fly over U.S. territory to reduce the likelihood of foreign air carriers incurring costly flight diversions resulting from passengers on-board who match the No Fly List.
Passenger checkpoint screening	DHS took steps to enhance passenger checkpoint screening through the implementation of standard operating procedures and the use of advanced imaging technology[e] and behavioral indicators. However, a risk-based strategy, a cost-benefit analysis of technologies, and a comprehensive validation of the science supporting TSA's behavioral analysis program are needed to improve efforts.	**DHS established passenger checkpoint screening standard operating procedures and expanded deployment of advanced imaging technology, but a risk-based strategy and a cost-benefit analysis of technologies would improve efforts.** **Key progress:** Passenger checkpoint screening is comprised of personnel who operate the checkpoint, standard operating procedures that screeners are to follow to conduct screening, and technology used during screening. TSA developed and implemented passenger checkpoint screening standard operating procedures and technologies. In making modifications to passenger checkpoint screening standard operating procedures, TSA considered the daily experiences of airport staff, complaints and concerns raised by the traveling public, and analysis of risks to the aviation system. TSA also made efforts to balance the impact on security, efficiency, and customer service when deciding which modifications to implement. In addition, TSA completed a strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies, and tested and deployed technologies to strengthen checkpoint screening. More recently, in response to the December 25, 2009, attempted attack on Northwest flight 253, TSA 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, and using advanced imaging technology as a primary—instead of a secondary—screening measure where feasible.[f] In July 2011, TSA reported that there were 488 advanced imaging technology units deployed at 78 airports throughout the United States.[g] TSA also reported that it is investing in new software for the units to enhance privacy by eliminating passenger-specific images and indicating potential threat items on a generic outline of a person. TSA plans to install this new software on every currently deployed unit in the fall of 2011.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We identified work remaining in DHS's efforts to develop and deploy checkpoint technologies. For example, as we reported in October 2009, 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 set forth in DHS's *National Infrastructure Protection Plan*. Specifically, TSA's strategic plan did not reflect the principle of conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and developing a cost-benefit analysis and performance measures.[h] Furthermore, in October 2009, we reported that since the establishment of TSA in November 2001, 10 passenger screening technologies had been in various phases of research, development, test and evaluation, procurement, and deployment, but TSA had not deployed any of these technologies to airports nationwide. Technologies that have now been deployed to airports include advanced imaging technology, advance technology X-ray, and bottle liquid scanners. However, we reported problems with some of these technologies. For example, in March 2010, we reported that it was unclear whether the advanced imaging technology would have detected the weapon used in the December 2009 incident based on the preliminary testing information we received. We have made recommendations to DHS to strengthen its efforts to develop and implement screening technologies at passenger checkpoints. In October 2009, we recommended, among other things, that DHS (1) conduct a risk assessment and develop performance measures for passenger screening technologies, and (2) to the extent feasible, ensure that technologies have completed operational tests and evaluations before they are deployed. DHS concurred with these recommendations and took steps to address them, such as working to develop a Risk Management and Analysis Toolset, to simulate the potential of some technologies to reduce the risk of certain threat scenarios which will apply specifically to the passenger screening process. In addition, we recommended that DHS conduct a cost-benefit analysis of technologies. DHS concurred and reported that it is currently finalizing a cost-benefit analysis for the advance imaging technology, for example. As we reported in March 2010, cost-benefit analyses are important because they help decision makers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk with available resources. As TSA is in the process of finalizing its cost-benefit analysis, it is too early to assess its results.

Area	Overall assessment	Summary of key progress and work remaining
		TSA has utilized behavioral indicators to identify persons who pose a risk to aviation security, but TSA has not yet fully validated the science supporting its behavior detection techniques. **Key progress:** As we reported in May 2010, TSA is screening passengers using TSA staff trained in behavior detection principles. TSA deployed about 3,000 Behavior Detection Officers to 161 airports as part of its Screening of Passengers by Observation Techniques program, at an annual cost of over $200 million. If TSA receives its requested appropriation for fiscal year 2012, TSA would be in a position to have invested about $1 billion in the program since fiscal year 2007. In May 2010, we reported that TSA had not validated the science supporting the program or determined if behavior detection techniques could be successfully used across the aviation system to detect threats before deploying the program. We recommended, among other things, that TSA convene an independent panel of experts to review the methodology of a study that the DHS Science and Technology Directorate was conducting on the program to determine whether the study's methodology was sufficiently comprehensive to validate the program. DHS concurred and stated that its validation study, completed in April 2011, included an independent review of the study with input from a broad range of federal agencies and relevant experts, including those from academia. DHS's validation study found that the program was more effective than random screening to varying degrees. However, the study identified that more work was needed to determine whether the science can be used for counterterrorism purposes in the aviation environment. The DHS study made recommendations related to strengthening the program and conducting a more comprehensive validation of the science for use in the aviation environment. TSA is reviewing the study's findings and assessing the steps needed to address DHS's recommendations. **What remains to be done:** Given that DHS's validation study was not designed to fully validate whether behavior detection can be used to reliably identify individuals who pose a security risk in an airport setting, it is not clear whether this program is the most effective use of TSA's resources.
Checked baggage screening	Through its Electronic Baggage Screening Program, TSA developed and deployed systems for screening checked baggage, but needs a plan for updating its explosives detection systems.	**TSA developed and deployed systems to screen checked baggage, but lacks a plan for updating its explosives detection systems.** **Key progress:** TSA's Electronic Baggage Screening Program—which facilitates the development and deployment of optimal checked baggage screening solutions to the nation's airports—is one of the largest acquisition programs in DHS. TSA uses two types of technology for checked baggage screening—the explosives detection system (in both in-line and stand-alone configurations) and the explosives trace detection machine—at the over 460 U.S. commercial airports. Optimal airport solutions may consist of explosives detection systems in either the in-line or stand-alone configuration, or explosives trace detection machines, depending on airport size and other factors. In January 2010, TSA revised explosives detection system requirements to better address current threats and plans to implement these requirements in a phased approach.

Area	Overall assessment	Summary of key progress and work remaining
		In March 2005, we reported that airports benefit from the installation of more efficient systems, such as in-line baggage screening systems, because these systems reduce the time needed for baggage screening and allow airports and TSA to streamline their operations. We also reported that TSA had not conducted a systematic, prospective analysis to determine at which airports it could enhance efficiencies and security by installing more efficient in-line systems. We recommended that TSA, among other things, identify and prioritize the airports where the benefits of optimizing baggage screening operations by replacing existing baggage screening systems with more efficient in-line systems were likely to exceed the estimated up-front investment costs of installing the systems, or where the systems were needed to address security risks. TSA concurred with this recommendation and published a plan to deploy more efficient systems for 250 airports. In January 2011, TSA reported that it plans to complete its efforts to replace or modify systems at these airports by 2024. In addition, TSA reported in July 2011 that over the next 5 years it intends to shift its focus from completion of optimal airport systems to the replacement of the aging explosives detection systems equipment. TSA is currently working to finalize a recapitalization and optimization strategic plan to prioritize airports' checked baggage screening equipment needs based upon a combination of the age of equipment and maintenance data. We have ongoing work examining, in part, the extent to which TSA has deployed optimal screening systems at commercial airports.[i] We plan to report on the final results of our work later this year. **What remains to be done:** We identified work remaining in TSA's efforts to screen checked baggage. For example, in July 2011 we reported that TSA faced challenges in procuring the first 260 explosives detection systems to meet TSA's revised 2010 explosives detection systems requirements, which expanded the number and types of explosives that explosives detection systems must detect. Also, TSA had not developed a plan to procure explosives detection systems to meet subsequent phases of the 2010 requirements. In July 2011, we recommended that TSA develop a plan to ensure that new machines, as well as those machines currently deployed in airports, will be operated at the levels in established requirements, and develop a reliable schedule for the Electronic Baggage Screening Program. DHS concurred with these recommendations and has begun taking action to address them, for example, by convening a working group to prepare a plan to procure any additional required technology, and to ensure that a capability gap does not arise from using new explosives detection systems in conjunction with existing explosives trace detection machines. DHS expects to finalize this plan by the fourth quarter of fiscal year 2012. Until TSA develops a plan identifying how it will approach the upgrades for currently deployed explosives detection systems—and the plan includes such items as estimated costs and the number of machines that can be upgraded—it will be difficult for TSA to provide reasonable assurance that its upgrade approach is feasible or cost-effective. Further, while TSA's efforts are positive steps, as TSA does not intend to finalize its plan until fiscal year 2012, it is too early to assess its impact.

Area	Overall assessment	Summary of key progress and work remaining
Air cargo security	TSA took steps to implement its air cargo security functions, but does not have a data verification mechanism and approved technologies for screening air cargo transported on pallets or in containers.	**TSA took steps to implement its air cargo security functions, but does not have a data verification mechanism and approved technologies for screening air cargo transported on pallets or in containers.** **Key progress:** The Implementing Recommendations of the 9/11 Commission Act of 2007 mandated that DHS establish a system to screen 100 percent of cargo flown on passenger aircraft—including the domestic and inbound flights of foreign and U.S. passenger operations—by August 2010.[j] TSA 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 in accordance with the mandate. TSA took several actions in meeting this mandate as it applied to domestic cargo, including creating a voluntary program to facilitate screening throughout the air cargo supply chain and taking steps to test technologies for screening air cargo. TSA also took steps to enhance the security of inbound air cargo (cargo bound for the United States), but has not yet fulfilled this portion of the statutory mandate. In January 2011, DHS asked passenger carriers to comment on their ability to screen 100 percent of air cargo on international inbound passenger aircraft by December 31, 2011. As of July 2011, TSA reported that it was reviewing carrier feedback and will use this feedback to help finalize the agency's strategy and timeline for implementing the 100 percent inbound air cargo screening requirement. As part of this effort, TSA reported that the agency will work with industry and foreign government partners to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process, which recognizes foreign government air cargo security programs that TSA determines provide a level of security commensurate with U.S. air cargo security standards. TSA also took steps to enhance the security of inbound air cargo following the October 2010 Yemen air cargo bomb attempt—such as requiring additional screening of high-risk air cargo prior to transport on an all-cargo aircraft. **What remains to be done:** We identified work remaining in TSA's efforts to develop and implement air cargo screening policies and procedures and questioned whether TSA would be able to effectively screen inbound air cargo by the end of 2011, as TSA estimated, given limitations in technology and screening data. In June 2010 we reported that TSA did not have a mechanism to verify the accuracy of domestic and inbound air cargo screening data. Further, there was no technology approved or qualified by TSA to screen cargo once it is loaded onto a unit-load device pallet or container—both of which are common means of transporting air cargo on wide-body passenger aircraft, thus requiring that screening occur before incorporation into pallets and containers. We made a number of recommendations to DHS to strengthen air cargo screening. For example, in June 2010, we recommended that TSA develop a mechanism to verify the accuracy of all screening data, both self-reported domestic and inbound data for cargo transported on passenger aircraft, through random checks or other practical means. TSA partially concurred and has actions underway to address this recommendation, noting that while current screening percentages are based on actual data reported by air carriers, verifying the accuracy of the screening data is difficult. However, TSA is not yet positioned to verify the accuracy of screening data. Verifying industry-reported screening data should better position TSA in providing reasonable assurance that screening is being conducted at reported levels. We are continuing to review these issues and plan to report on our results early next year.[k]

Area	Overall assessment	Summary of key progress and work remaining
Security of airports	TSA implemented various activities to strengthen security of airports, such as assessing risks to airport perimeters, establishing access controls to secure areas of airports, and expanding requirements for worker background checks. However, an evaluation plan for pilot tests to screen workers would improve these efforts.	**TSA strengthened airport security, such as assessing risks to airport perimeters. However, efforts should be further enhanced by establishing an evaluation plan for pilot tests to screen workers.** **Key progress:** In September 2009, we reported that TSA used several means to identify and assess potential threats to airport security, such as daily intelligence briefings, weekly suspicious incident reports, and situational awareness reports, all of which are available to internal and external stakeholders. TSA also issues an annual threat assessment of the U.S. civil aviation system, which includes an assessment of threats to airport perimeter and access control security. According to TSA officials, these products collectively formed TSA's assessment of threats to airport perimeters and access controls. Additionally, TSA took steps to enhance airport security by expanding its requirements for conducting worker background checks and implementing a random worker screening program. **What remains to be done:** We identified several challenges to strengthening security of airports. For example, we reported in September 2009 that TSA had implemented activities to assess risks to airport perimeters and access controls. We also reported that TSA had conducted joint vulnerability assessments (assessments conducted jointly by TSA and the Federal Bureau of Investigation) at about 13 percent of the approximately 450 commercial airports nationwide, at that time. We also reported, however, that such assessments had not been conducted at 87 percent of the nation's commercial airports and that TSA had not conducted any consequence assessments. As we noted in our 2009 report, TSA officials said that they did not know to what extent the 87 percent of commercial airports, most of which were smaller airports, were vulnerable to an intentional security breach. In July 2011, we reported that joint vulnerability assessments had not been conducted at 83 percent of the nation's airports. In July 2011, TSA told us that plans are being developed to conduct joint vulnerability assessments at more airports as deemed appropriate. Additionally, TSA reported that TSA's national inspection program requires that transportation security inspectors conduct vulnerability assessments at all commercial airports, which are based on the joint vulnerability assessment model. According to TSA, every commercial airport in the United States receives a security assessment every year, including an evaluation of perimeter security and access controls. As we noted in our 2009 report, TSA identified joint vulnerability assessments, along with professional judgment, as the agency's primary mechanism for assessing airport security vulnerabilities in accordance with *National Infrastructure Protection Plan* requirements. We have not yet assessed the extent to which transportation security inspectors consistently conduct vulnerability assessments based on the joint vulnerability model as TSA stated.

Area	Overall assessment	Summary of key progress and work remaining
		Further, in September 2009, we reported that significant limitations in TSA's design and evaluation of pilot tests to screen airport workers, such as the limited number of participating airports—7 out of about 450, at the time—made it unclear which method was most cost-effective. In addition, we reported that TSA's efforts were not guided by a unifying national strategy that identified key elements, such as goals, priorities, performance measures, and required resources. We made recommendations to TSA to strengthen airport perimeter security and access controls. For example, we recommended in September 2009 that TSA develop a comprehensive risk assessment of airport security and evaluate the need to conduct an assessment of security vulnerabilities at airports nationwide. DHS concurred and said, for example, that it would include an assessment of airport perimeter and access control security risks as part of a comprehensive assessment for the transportation sector, which DHS did in the *Transportation Sector Security Risk Assessment*, published in July 2010. This document included an assessment of various risk-based scenarios related to airport perimeter security but did not consider the potential vulnerabilities of airports to an insider attack—the insider threat—which DHS recognized as a significant issue. In July 2011, TSA officials told us that the agency was developing a framework for insider risk that is to be included in the next iteration of the assessment, which TSA expected to be released at the end of calendar year 2011. Such action, if taken, would meet the intent of our recommendation. We further recommended that DHS ensure that future airport security pilot programs include a well-developed evaluation plan. TSA concurred with this recommendation, and in August 2011 reported that, because it has no current plans to conduct another pilot program, it has not yet taken action to address this recommendation. Additionally, we recommended that TSA develop a national strategy for airport security that incorporates key characteristics of effective security strategies, such as measurable goals and priorities. DHS concurred and stated that it would update its Transportation Systems-Sector Specific Plan to include these characteristics. TSA provided a copy of the updated plan to congressional committees in June 2011 and to us in August 2011. We reviewed this plan and its accompanying aviation model annex and found that while the plan provided a high-level summary of program activities for addressing airport security such as the screening of workers, the extent of which these efforts would be guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address the intent of our recommendation.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] See, e.g., Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, § 522(a), 118 Stat. 1298, 1319 (2004) (setting forth 10 statutory conditions that DHS must have satisfied before deploying or implementing the passenger prescreening program that is today referred to as Secure Flight).

[b] In addition to TSA's Secure Flight program, CBP also screens passengers on all flights arriving in and departing from and within the U.S. prior to boarding a flight or vessel. This review process starts up to 72 hours prior to departure through scrutiny of airline Passenger Name Records, provided through agreements with the carriers. On the day of departure, when an individual checks in for the intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP.

[c] Enplanements are the number of passengers who board a plane. We did not independently verify the accuracy of these data.

[d] We did not independently verify the accuracy of these data.

[e] Advanced imaging technology produces an image of a passenger's body that TSA personnel use to look for anomalies, such as explosives and other prohibited items.

[f] Passengers undergo either primary and, if circumstances warrant, secondary screening at passenger checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport, and involves passengers walking through a metal detector and their carry-on items being subjected to X-ray screening. Secondary screening is conducted on selected passengers and involves additional screening of both passengers and their carry-on items.

[g] We did not independently verify the accuracy of these data.

[h] Risk is a function of three elements: (1) threat—the probability that a specific type of attack will be initiated against a particular target/class of targets, (2) vulnerability—the probability that a particular attempted attack will succeed against a particular target or class of targets, and (3) consequence—the expected worst case or worst reasonable adverse impact of a successful attack.

[i] We are conducting our work for the Senate Committee on Commerce, Science, and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and Representative Henry C. Johnson, Jr.

[j] See 49 U.S.C. § 44901(g).

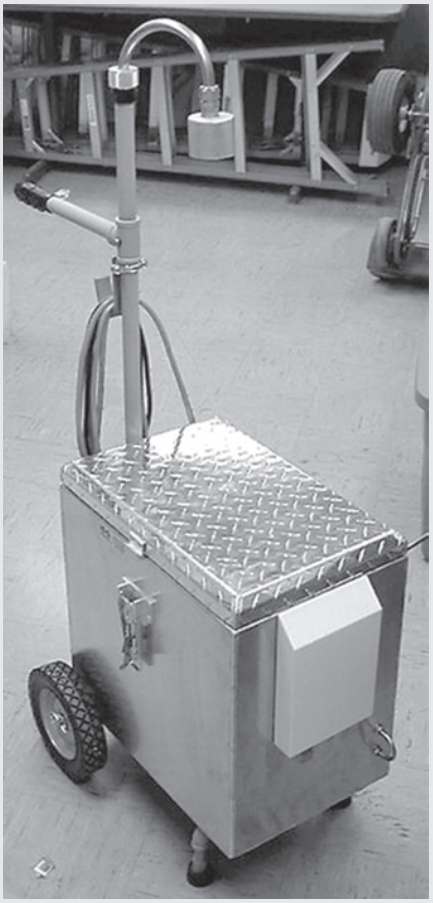
[k] We are conducting our work for the House Committee on Homeland Security, the House Subcommittee on Transportation Security, and the Senate Committee on Homeland Security and Governmental Affairs.

GAO Contact

For additional information about this area, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

Appendix IV: Chemical, Biological, Radiological, and Nuclear Threats

What This Area Includes



Source: DHS.

BioWatch Aerosol Collector.

The Department of Homeland Security (DHS) leads federal interagency coordination and planning for emergency response to catastrophic events such as chemical, biological, radiological, and nuclear (CBRN) incidents in the United States, and is responsible for assessing the risks posed by various CBRN agents. These efforts include (1) assessing risks, and (2) developing and deploying capabilities to detect and mitigate CBRN threats. Within DHS, the Science and Technology Directorate (S&T) is responsible for developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for identifying priorities, goals, objectives and policies for, and coordinating the federal government's civilian efforts to identify and develop countermeasures to chemical and biological threats.[1] The Domestic Nuclear Detection Office (DNDO) is responsible for developing, acquiring, and supporting the deployment of a system to detect and report on attempts to develop, transport, or use unauthorized nuclear explosive, fissile, or radiological materials or explosives in the United States. The Office of Health Affairs provides health and medical expertise in support of the DHS mission to prepare for, respond to, and recover from all threats, and leads and coordinates the department's biological and chemical defense activities.

For fiscal year 2011, S&T had about 450 personnel and budget authority of about $830 million. For fiscal year 2011, DNDO had about 130 personnel and budget authority of approximately $340 million. For fiscal year 2011, the Office of Health Affairs had about 95 personnel and budget authority of approximately $140 million. Chemical, biological, radiological, and nuclear threats assessment, detection, and mitigation primarily falls within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has developed and implemented other efforts related to CBRN assessments and detection and mitigation capabilities on which we are not reporting. For example, DHS has initiated efforts related to incidents involving contaminated debris, biodefense exercises and notification procedures for biological attacks. Further, in August 2011 DHS reported to us that it had (1) developed a

[1] 6 U.S.C. § 182(2).

strategic plan and issued guidance for biological threat prevention and response; (2) established a steering committee for anthrax preparedness and response; and (3) established a program that is developing best practices guidance and decision support tools for federal, state, and local stakeholders for preparedness and response to high consequence chemical incidents. DHS also reported launching a National Nuclear Forensics Expertise Development Program in fiscal year 2008 to enhance academic programs and expertise development opportunities in nuclear forensics. Moreover, DHS reported that it was leading development of a national strategic plan for improving nuclear forensics capabilities in the United States. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work has shown that DHS made progress in assessing risks posed by CBRN threats, developing CBRN detection capabilities, planning for nuclear detection, and conducting radiation detection. However, important efforts related to these areas have not been completed. For example, DHS conducted risk assessments for CBRN agents, but should better coordinate with the Department of Health and Human Services by developing written policies and procedures governing development of the assessments. DHS also developed the BioWatch program, which provides early detection of biological threats. However, the next generation of the system, which is to have additional detection capability, has not yet been operationally deployed. Further, DHS established the National Biosurveillance Integration Center, but the center lacks resources necessary for operations, such as data and personnel from its partner agencies. In August 2011, DHS reported that, among other actions, its Office of Health Affairs had begun to develop a new strategy for the Center. DNDO 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 DHS made progress in deploying radiation detection equipment. However, work remains in implementing the global nuclear detection strategy, and DHS faced difficulties in developing new technologies to detect radiological and nuclear materials. For example, DHS's strategic plan for the global nuclear detection architecture addressed some key components of what we previously recommended be included in a strategic plan, such as identifying the roles and responsibilities for meeting strategic objectives. However, the plan did not identify funding needed to achieve the strategic plan's objectives, or employed monitoring mechanisms for determining programmatic progress and identifying needed improvements. Table 8

provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 8: Assessment of Progress and Work Remaining in Key CBRN Threats Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
CBRN risk assessments	DHS conducted CBRN risk assessments, but should improve its coordination with agencies by developing procedures for developing the assessments.	**DHS assessed risks posed by CBRN threats, but should strengthen these efforts through improved interagency collaboration by developing written procedures for development of risk assessments.** **Key progress:** The May 2010 National Security Strategy noted that the American people face no greater or more urgent danger than a terrorist attack with a nuclear weapon, as well as the concern that the effective dissemination of a lethal biological agent within a U.S. city would endanger the lives of hundreds of thousands of people and would have unprecedented consequences. Both risk assessment and early detection are elements of assessing the potential for such an attack and its consequences. We reported in June 2011 that DHS develops risk assessments of CBRN threats and had issued seven classified CBRN risk assessments since 2006.[a] We also reported that DHS 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. As of June 2011, DHS had conducted 17 material threat assessments, each of which assessed the threat posed by a given CBRN agent or class of agents and the potential numbers of human exposures in plausible, high-consequence scenarios. **What remains to be done:** In June 2011 we reported that although DHS and the Department of Health and Human Services had coordinated with each other and with other federal departments to develop the CBRN risk assessments and material threat assessments, neither department had written procedures or interagency agreements for developing these assessments. In addition, we found that DHS's processes and coordination on the development of such assessments had varied, and reported that Health and Human Services officials stated they would like to be more involved. We recommended that DHS establish time frames and milestones to better ensure timely development and interagency agreement on written procedures for the development of DHS's CBRN risk assessments. DHS concurred and stated that it has begun developing a Strategic Implementation Plan for conducting the assessments. Developing a strategic implementation plan should help DHS better ensure timely development of risk assessments, but since this plan is in development, it is too early to assess its effectiveness.

Area	Overall assessment	Summary of key progress and work remaining
Development and deployment of CBRN detection and mitigation capabilities	DHS made progress related to the development and deployment of both biological and radiation detection equipment. However, more work remains to enhance collaboration and implement the global nuclear detection architecture.	**DHS made progress in the early detection, warning, and analysis of biological threats through its BioWatch program and the National Biosurveillance Integration Center; however, challenges remain in the clarity of roles and responsibilities related to biosurveillance efforts.** **Key progress:** To detect specific airborne biological threat agents, DHS implemented the BioWatch program, which monitors air samples in more than 30 metropolitan areas and, according to DHS, supports National Special Security Events. The Implementing Recommendations of the 9/11 Commission Act of 2007 established, within DHS, the National Biosurveillance Integration Center, with a mission of, among other things, enhancing the capability of the federal government to rapidly identify, characterize, localize, and track biological events of national concern.[b] The National Biosurveillance Integration Center was to help provide early detection and situational awareness by integrating information and supporting an interagency biosurveillance community. In December 2009, we reported that the Center made efforts to acquire data from its federal partners, obtain analytical expertise from other agencies, establish governance bodies to develop and oversee the community of federal partners, and provide information technologies to support data collection, analysis, and communication. **What remains to be done:** DHS reported that it was developing new detection technology, known as Generation 3.0, beginning in June 2008, which would replace the existing BioWatch technology and would provide a fully automated detector that both collects air samples and analyzes them for threats. In particular, DHS reported that the Generation 3.0 system improves detection times, increases population coverage, and provides greater cost effectiveness. We reported in December 2009 that the National Biosurveillance Integration Center, within DHS's Office of Health Affairs, was not fully equipped to carry out its mission because it lacked key resources, including data and personnel, from its partner agencies, with only 2 of 11 partner agencies having assigned personnel to the Center. In interviews with partner agencies, we found widespread confusion, uncertainty, and skepticism about the value of participation in the Center, as well as the mission and purpose of the Center within its community of federal partners. We noted that for the Center to obtain the resources it needs to meet its mission, it must effectively employ collaborative practices, and we recommended that the Center work with its interagency advisory body to develop a strategy for addressing barriers to collaboration, such as the lack of clear mission, roles, and procedures, and to develop accountability mechanisms to monitor these efforts. DHS concurred and, as of March 2011, reported that it was working to develop a collaboration strategy and performance measures. DHS reported that in August 2010, the Office of Health Affairs had initiated a review of the Center to enhance its ability to identify, characterize, localize, and track biological events of national concern. In addition, DHS is working with the Institute of Medicine to develop a report by the summer 2011 to help inform its strategy and define biosurveillance key terms, such as the mission, roles, and responsibilities. As DHS is working to implement these efforts, it is too early to assess their results.

Area	Overall assessment	Summary of key progress and work remaining
		DNDO coordinated the development of a strategic plan for the global nuclear detection architecture, but work remains in implementing the global nuclear detection strategy, and DHS faced difficulties in developing new technologies to detect radiological and nuclear materials. **Key progress:** Since December 2010, DNDO has coordinated the development of an interagency strategic plan to guide the development of the global nuclear detection architecture—the overall mission of the architecture is to protect against terrorist attacks using nuclear and radiological materials through coordinated detection, analysis, and reporting of the unauthorized importation, possession, storage, transportation, development, or use of such materials—and an annual report on the current status of the architecture.[c] **What remains to be done:** In July 2011, we testified that DHS's strategic plan addressed some key components of what we previously recommended be included in a strategic plan, such as identifying the roles and responsibilities for meeting strategic objectives. However, we found that neither the plan nor the annual report identified funding needed to achieve the strategic plan's objectives, or employed 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. As DHS has not yet issued this plan, we could not assess the extent to which it will address the elements we identified. In addition, since 2006 we have reported on difficulties faced by DHS in developing new technologies to detect nuclear and radiological materials. Specifically, we have reported on longstanding problems with DNDO's efforts to deploy advanced spectroscopic portal radiation detection monitors. The spectroscopic portal radiation detection monitors are a more advanced and significantly more expensive type of radiation detection portal monitor to replace the existing polyvinyl toluene portal monitors in many locations that the U.S. Customs and Border Protection (CBP) currently uses to screen cargo at ports of entry. We have issued numerous reports regarding problems with the cost and performance of the advanced spectroscopic portal monitors and the lack of rigor in testing this equipment. For example, we found that tests DNDO conducted in early 2007 used methods that enhanced the apparent performance of advanced spectroscopic portal radiation detection monitors and did not use critical CBP operating procedures that were fundamental to the performance of current radiation detectors. In July 2011, DHS announced that DNDO and CBP would end development of the advanced spectroscopic portal monitors as originally conceived given the challenges the program has faced. However, DNDO reported to us that it plans to deploy 9 of the remaining already procured advanced spectroscopic portal machines at ports of entry, in addition to the 4 already deployed, to gather more complete data about operational needs.

Source: GAO analysis.

[a] DHS issued three bioterrorism risk assessments in 2006, 2008, and 2010; two chemical terrorism risk assessments in 2008 and 2010; and two integrated CBRN terrorism risk assessments in 2008 and 2011. DHS also plans to issue the first radiological and nuclear terrorism risk assessment in 2011.

[b] 6 U.S.C. § 195b.

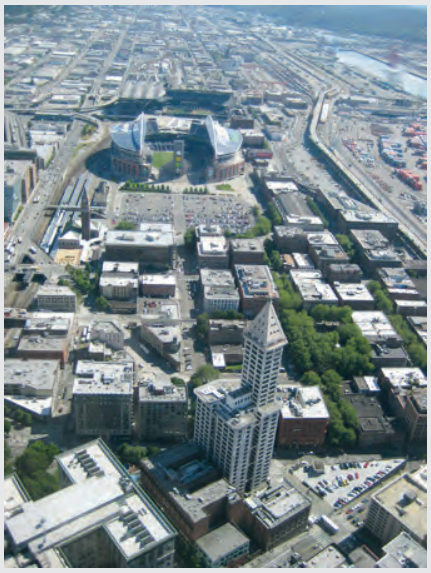
[c] The global nuclear detection architecture is a multi-departmental effort coordinated by DNDO, and the strategic plan establishes a broad vision for the architecture, identifies crosscutting issues, defines several objectives, and assigns mission roles and responsibilities to the various federal entities that contribute to the architecture.

GAO Contacts

For additional information about this area, contact William O. Jenkins, Jr. at (202) 512-8757 or jenkinswo@gao.gov, or Gene Aloise at 202-512-6870 or aloisee@gao.gov.

Appendix V: Critical Infrastructure Protection—Physical Assets

What This Area Includes



Source: GAO.

Downtown Seattle and Port Area.

Under the Homeland Security Act of 2002, the Department of Homeland Security (DHS) has wide-ranging responsibility to lead and coordinate the nation's efforts to secure critical infrastructure.[1] DHS's key responsibilities and efforts include (1) risk assessment and planning; (2) protection and resiliency; and (3) partnerships and coordination mechanisms. DHS leads and coordinates the nation's efforts to enhance protection and resiliency for 18 critical infrastructure sectors. Within DHS, three components are charged with lead responsibility over 11 of the 18 sectors.[2] Specifically, within DHS's National Protection and Programs Directorate (NPPD), the Office of Infrastructure Protection is responsible for the chemical; commercial facilities; critical manufacturing; dams; emergency services; and nuclear reactors, materials, and waste sectors. Also within NPPD, the Office of Cybersecurity and Communications is responsible for the communications and information technology sectors, and the Federal Protective Service (FPS) is responsible for the government facilities sector. The Transportation Security Administration (TSA) is responsible for the postal and shipping sector and in turn shares responsibility with the U.S. Coast Guard for the transportation systems sector. As the primary component responsible for critical infrastructure protection via its Office of Infrastructure Protection, for fiscal year 2011 NPPD had about 2,800 personnel and its budget authority was about $2.3 billion.[3] Critical infrastructure protection of physical assets primarily falls within the

[1] Pub. L. No. 107-296, 116 Stat. 2135 (2002). Homeland Security Presidential Directive 7 further defined critical infrastructure protection responsibilities for DHS and those federal agencies responsible for particular critical infrastructure sectors, such as the chemical, commercial facilities, energy, and transportation sectors. The Directive also directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

[2] In addition to DHS, the other federal agencies that serve as sector-specific agencies include the Department of Defense, which is responsible for the defense industrial base sector; the Environmental Protection Agency, which is responsible for the water sector; the Department of Agriculture and the Food and Drug Administration, which are responsible for the food and agriculture sector; and the Department of Interior, which is responsible for the national monuments and icons sector.

[3] The resource amounts provided here encompass resources for all NPPD programming, including programs which do not focus on critical infrastructure protection and resiliency efforts, such as the U.S. Visitor and Immigrant Status Indicator Technology program, which focuses on providing biometric identification services. According to DHS, NPPD's budget authority for fiscal year 2011 included $1.3 billion in appropriated funds and the authority to acquire another $1.1 billion in fees for FPS. These values do not add up to $2.3 billion due to rounding.

Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has developed and implemented other efforts related to critical infrastructure protection on which we are not reporting. For example, according to DHS, it is currently developing measures for critical infrastructure protection and resiliency as part of its efforts to develop the National Preparedness Goal and National Preparedness System directed by Presidential Policy Directive 8: National Preparedness. DHS stated that as part of this effort, it is examining the extent to which these measures incorporate crosscutting considerations such as sustainability, durability, and energy efficiency. As these efforts relate to critical infrastructure protection, we have not completed work on them upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the DHS IG's work, has shown that DHS expanded its efforts to conduct risk assessments and planning, provide for protection and resiliency, and implement partnerships and coordination mechanisms for physical critical assets. 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 an enhanced discussion about DHS risk management. Also, in the *National Infrastructure Protection Plan*, DHS expanded the discussion of its program to prioritize assets and systems for each of the 18 sectors according to their importance, nationally or regionally. Further, DHS took steps to coordinate with critical infrastructure protection stakeholders through information sharing mechanisms such as council meetings. However, our work and that of the DHS IG has shown that key challenges remain in these areas. For example, DHS's state and local partners who are to provide data for the development of annual lists of critical infrastructure assets and systems noted that time and resource constraints can adversely affect the process. Furthermore, 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, the scope of some risk assessments has been limited and assessment results have not been consistently incorporated into planning efforts. In addition, DHS should take additional action to address barriers faced in sharing

information about resiliency strategies with critical infrastructure partners. Table 9 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 9: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Physical Assets Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS updated the *National Infrastructure Protection Plan* to include an emphasis on resiliency and an expanded discussion on identifying and prioritizing critical infrastructure. DHS components responsible for specific sectors have used risk-based assessments to enhance critical infrastructure planning and protection; however, the scope of some assessments has been limited and assessments' results have not been consistently incorporated into planning efforts.	**DHS made revisions to the *National Infrastructure Protection Plan* to include an emphasis on resiliency.** **Key progress:** In accordance with the Homeland Security Act and in response to Homeland Security Presidential Directive 7, DHS issued, in June 2006, the first *National Infrastructure Protection Plan*, which provided the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. DHS issued a revised *National Infrastructure Protection Plan* in January 2009 to include updates to critical infrastructure protection planning.[a] In March 2010, we reported that the revised plan incorporated an increased emphasis on resiliency by treating resiliency on an equal footing with protection.[b] DHS also updated the plan's discussion of DHS's overall risk management framework based on stakeholder input and sectors' experiences performing critical infrastructure protection activities, and increased its emphasis on regional planning. Further, DHS made changes regarding how sectors are to measure the performance of their critical infrastructure protection programs. The 2009 plan also included an additional discussion regarding the development of metrics that assess how well programs reduced the risk to the sector. Additionally, according to DHS, beginning in 2011 sectors are expected to report progress against risk-based outcome statements and metrics in the Sector Annual Reports—a progress report called for by Homeland Security Presidential Directive 7. DHS also stated that it plans to collaborate with the sectors to develop a plan for addressing crosscutting opportunities for improvement in critical infrastructure protection and resiliency.
		DHS's efforts to enhance its ability to identify and prioritize critical infrastructure is evolving. **Key progress:** DHS identifies and prioritizes nationally significant critical assets, systems, and networks to determine which of these face the highest risk, establish risk management priorities, and help inform planning and resource decisions. In March 2010 we reported that DHS's update to the *National Infrastructure Protection Plan* provided an expanded discussion about how DHS identifies and prioritizes critical infrastructure. Specifically, in contrast to the 2006 plan, the 2009 plan included a more detailed discussion of the national critical infrastructure prioritization program that places critical infrastructure into categories according to their importance, nationally or regionally.

Area	Overall assessment	Summary of key progress and work remaining
		Further, in June 2009, the DHS IG reported that DHS had worked with state homeland security partners to compile annual lists of critical assets and systems and had begun to use consequence-based criteria focused on assets and systems whose disruption could have either catastrophic national consequences or nationally significant consequences. The DHS IG reported that the creation of these lists was complex and difficult for several state partners. For example, the DHS IG reported that (1) some DHS partners noted that time and resource constraints can adversely affect their ability to participate in the data compilation process, and (2) the strength of state critical infrastructure programs varied across the nation, impeding some partners' ability to provide timely and comprehensive information. The DHS IG recommended ways that DHS should enhance partner participation in the list development process and obtain additional resources to enhance asset and system identification efforts. DHS generally concurred and addressed the recommendations. According to DHS, it addressed these recommendations through actions such as developing unclassified lists to provide state level homeland security officials access to information about infrastructure assets and systems critical to their jurisdictions, and leading a national critical infrastructure prioritization program working group to discuss program enhancements with sector partners. Later this year, we plan to begin work for the Senate Committee on Homeland Security and Governmental Affairs; House Committee on Homeland Security and the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies examining recent DHS efforts to identify and prioritize critical infrastructure.
		DHS components responsible for specific sectors have begun to use risk-based assessments in critical infrastructure planning and protection, but face challenges in conducting these assessments and should enhance incorporation of their results into planning. **Key progress:** DHS components with responsibility for critical infrastructure sectors have begun to use risk-based assessments in their critical infrastructure related planning and protection efforts, but they have faced implementation challenges. For example, in April 2010, we reported that the Coast Guard used its Maritime Security Risk Analysis Model to help concentrate maritime security activities when and where relative risk is believed to be the greatest. The Model is used to assess the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios—such as the risk to ferries associated with a suicide bomber or a boat attack—consistent with the risk management framework established in the *National Infrastructure Protection Plan*. Also, according to the Coast Guard, the Maritime Security Risk Analysis Model is designed to support national decision making and long term strategic planning, evaluate capabilities needed to combat future terrorist threats, and identify the highest-risk scenarios and targets in the maritime domain. Further, we reported in March 2009 that TSA took action to implement a risk management framework across the surface transportation sector. We issued a series of reports on surface transportation security that found, among other things, that TSA had issued modal strategies intended to guide its efforts to secure the various surface transportation modes. Further, according to TSA, in 2010, it developed risk assessments for highway infrastructure and the trucking and the school bus industries, among others, that were incorporated into the *Transportation Sector Security Risk Assessment*.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We have identified weaknesses in DHS components' efforts to implement risk-based assessments in enhancing critical infrastructure planning and protection. For example, we reported that TSA's efforts to conduct threat, vulnerability, and consequence assessments within the individual surface transportation modes had limitations. In April 2009, we reported that TSA's efforts to assess risk to freight rail had primarily focused on one key threat (rail shipments of certain highly toxic materials), although other federal and industry assessments had identified additional potential security threats, including risks to critical infrastructure. In addition, in January 2009, we reported that TSA's strategy for securing the highway mode was not based on completed risk assessments. For example, while nearly all of TSA's and the Office of Infrastructure Protection's available vulnerability assessments were conducted prior to the issuance of the highway security strategy, their results were not used to develop the strategy. We recommended, among other things, that TSA conduct risk assessments that combined threat, vulnerability, and consequence to help produce a comparative assessment within the transportation modes and across the transportation sector—a tool that could also be used for current and future investment decisions. TSA concurred, and in June 2010 TSA produced the *Transportation Sector Security Risk Assessment*, which assessed risk within and across the various transportation modes. TSA expects to complete an enhanced version of the risk assessment at the end of calendar year 2011 to help address limitations it identified in the 2010 assessment.[c] Thus, it is too early to assess the effectiveness of this assessment. In July 2011, TSA also reported developing a methodology for the identification and assessment of critical freight rail infrastructure, such as bridges and tunnels, which includes factors that account for vulnerability and consequence. TSA stated that it uses the results of these assessments to prioritize both railroad infrastructure hardening projects and grants. Further, DHS provided its updated transportation security strategy to congressional committees in June 2011 and to us in August 2011. However, we have not yet assessed the extent to which it addresses our recommendations, as the strategy was recently issued. In addition, we identified challenges that FPS faces in implementing a risk-based staffing plan for protecting federal facilities. For example, in 2009 we reported that, among other things, FPS's workforce planning was limited because FPS headquarters did not collect data on its workforce's knowledge, skills, and abilities. Without such information, we reported that FPS was not able to determine what its optimal staffing levels should be or identify gaps in its workforce needs, and determine how to modify its workforce planning strategies to fill these gaps. FPS drafted a staffing plan in June 2010, consistent with our recommendation. According to FPS, the agency is working to finalize its staffing plan, which has been approved by the Secretary of Homeland Security and provided to the Office of Management and Budget before being submitted to the Secretary of Homeland Security for final approval. As this staffing plan has not yet been finalized, it is too soon to assess its results. Such a plan is needed to help FPS determine what its optimal staffing levels should be, to identify gaps in its workforce needs, and to determine how to modify its workforce planning strategies to fill these gaps.

Area	Overall assessment	Summary of key progress and work remaining
Protection and resiliency	DHS's efforts to assess protection and resiliency are evolving and include actions to bring a stronger focus to resiliency. However, performance measures are needed to determine the extent to which actions are being taken to address resiliency gaps.	**DHS's efforts to assess protection and resiliency are evolving, but performance measurement should be strengthened.** **Key progress:** DHS has various voluntary programs in place to conduct vulnerability assessments and security surveys at and across facilities from the 18 sectors, and uses these assessments to develop and disseminate information on steps asset owners and operators can take to protect their facilities. In September 2010, we reported that consistent with the updated *National Infrastructure Protection Plan*, DHS had taken action to develop or enhance the programs it uses to work with asset owners and operators to bring a stronger focus to resiliency. For example, in 2009 DHS developed the Regional Resiliency Assessment Program to assess vulnerability, threats, and potential consequences associated with groups of related infrastructure, regions, and systems in major metropolitan areas. The program is intended to identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps, and to provide training and other assistance. DHS was also revising assessment tools used to assess vulnerabilities at individual facilities. **What remains to be done:** In September 2010 we reported that DHS had not developed an approach to measure its effectiveness in working with asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during the various vulnerability assessments. We recommended that DHS develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during these assessments. DHS agreed and has reported that it is taking actions to address the recommendation. According to DHS, these actions include developing performance measures related to the impact of Office of Infrastructure Protection assessments on improving the protection and resilience of critical infrastructure. They also include the development of a mechanism to assess the extent to which asset owners and operators are taking actions to enhance security and resilience with associated output metrics. We are currently conducting a review for the House Committee on Homeland Security assessing DHS's efforts to manage its vulnerability assessment programs, including its efforts to measure the actions owners and operators take to mitigate vulnerabilities identified by DHS. We plan to report on our results in 2012.
		DHS's Protective Security Advisor Program is intended to assist asset owners and operators on protection and resiliency issues. **Key progress:** DHS deployed 93 critical infrastructure protection and security specialists, called Protective Security Advisors, to local communities throughout the country to assist asset owners and operators in all 18 sectors on critical infrastructure protection strategies. In September 2010, we reported that DHS had begun to train the Protective Security Advisors about resiliency and how it applies to the owners and operators they interact with. However, we reported that DHS had not updated guidance that outlines the Protective Security Advisors' roles and responsibilities to reflect DHS's growing emphasis on resiliency. We recommended that DHS update the Protective Security Advisor guidance that discusses the role the Security Advisors play during interactions with asset owners and operators with regard to resiliency. DHS agreed and provided additional training and updated guidance to Protective Security Advisors on their role with regard to resiliency during their interactions with owners and operators.

Area	Overall assessment	Summary of key progress and work remaining
Partnerships and coordination mechanism	DHS took steps to coordinate with critical infrastructure stakeholders to address overlaps and gaps by clarifying roles and responsibilities for agencies that have regulatory oversight for critical infrastructure sectors. However, limited collaboration has hindered federal emergency communication efforts. In addition, DHS shares the results of vulnerability assessments with critical infrastructure partners, but has not developed an approach to disseminate information on resiliency practices within and across sectors.	**DHS took steps to coordinate with critical infrastructure stakeholders to identify security gaps and overlaps, but limited collaboration has hindered federal emergency communication efforts.** **Key progress:** In May 2011, we reviewed the coordination activities of nine critical infrastructure sectors to identify any security overlaps and gaps. While our findings are not generalizable to all 18 sectors, we found that DHS coordinated with critical infrastructure stakeholders, including other federal regulatory authorities, through information-sharing mechanisms, such as council meetings, to identify overlaps and gaps in critical infrastructure security activities. In addition, DHS took action to address overlapping security activities by clarifying roles and responsibilities for critical infrastructure security activities with agencies that have regulatory oversight through coordination mechanisms, including memorandums of understanding and working groups. Furthermore, DHS developed and distributed tools, such as guides, to critical infrastructure sectors and conducted voluntary training and exercises to enhance security capabilities. DHS also conducted vulnerability assessments and security surveys at both public and privately owned facilities that volunteer for such efforts. We are beginning work for the House Committee on Homeland Security on DHS's voluntary programs and its efforts to measure the effectiveness of its voluntary programs in enhancing critical infrastructure protection and resiliency. We plan to report on our efforts in 2012. **What remains to be done:** We also reported on challenges that DHS faces in coordinating with federal partners. For example, in June 2009, we reported that, with respect to the communications sector, limited collaboration and monitoring by DHS and its federal partners hindered federal emergency communications efforts. Federal agencies had demonstrated limited use of some best practices that we previously reported as helpful for addressing issues like emergency communications, such as promoting a public safety network for emergency communications. We recommended, among other things, that DHS and its partners systematically track, assess, and respond to stakeholder groups' recommendations, including identifying opportunities to work with other agencies, as appropriate, to advance recommendations. DHS generally concurred with our recommendations and in response reported that it has taken steps toward addressing them, such as sharing the stakeholder groups' recommendations with the Emergency Communications Preparedness Center, a focal point and clearinghouse for implementing federal interoperable communications efforts. While these are positive steps, it is unclear how the Center would incorporate the work of stakeholder groups. Improved monitoring and accountability of stakeholder and advisory committee's recommendations would boost the value of these groups by monitoring agency responses, avoiding duplication of efforts, and identifying opportunities to work with other agencies.

Area	Overall assessment	Summary of key progress and work remaining
		DHS shares the results of vulnerability assessments with critical infrastructure partners, but has not developed an approach to disseminate information on resiliency practices within and across sectors. **Key progress:** DHS shares information on potential protective measures with various partners, such as asset owners and operators, and others including state and local officials (generally on a case-by-case basis) after it has completed vulnerability assessments at critical infrastructure facilities. Further, in September 2010 we reported that DHS relies on its private-sector partners to develop and share information on practices they use to enhance their protection and resilience. DHS officials said that the practices shared by sector partners, including best practices, were largely identified and developed by the private sector, at times with the support of its partners in government such as the sector-specific agencies. DHS facilitated this process by making various mechanisms available for information sharing, including information they deemed to be best practices. For example, according to senior DHS officials, DHS's Homeland Security Information Network-Critical Sectors was designed to provide each sector a portal to post useful or important information, such as activities or concepts that private-sector partners discern to be best practices on protection and resiliency topics. **What remains to be done:** DHS faces barriers to sharing information about resiliency strategies. For example, given the voluntary nature of the critical infrastructure partnership, DHS officials stated that DHS should not be viewed as identifying and promoting practices that could be construed by critical infrastructure partners to be standards. Also, according to DHS officials, the need for and the emphasis on resiliency can vary across different types of facilities depending on the nature of the facility. In our September 2010 report, we recognized that DHS faces barriers to information sharing. However, we concluded that as the primary federal agency responsible for coordinating and enhancing the protection and resiliency of critical infrastructure across the sectors, DHS is uniquely positioned to disseminate information on resiliency practices to help asset owners and operators consider and adopt resiliency strategies. Thus, we recommended, among other things, that DHS determine the feasibility of overcoming these barriers and developing an approach to disseminate resiliency information. DHS did not agree with the recommendation, but stated that it would expand the distribution of resiliency products to critical infrastructure stakeholders. In July 2011 DHS reported taking steps to address our recommendation, including disseminating documents related to protection and resiliency that cover some resiliency measures. DHS further reported that as its understanding of stakeholder needs in this area grows, it will be able to synthesize more focused resiliency products. These efforts should better position DHS for sharing resiliency information. However, as our work has shown, DHS needs to determine the feasibility of developing an approach to better disseminate resiliency practices to better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

[b] Our assessment of the two plans was limited to determining how the 2009 *National Infrastructure Protection Plan* changed compared to the 2006 plan, and how DHS and the sectors addressed resiliency as part of their planning efforts.

[c] TSA noted limitations in the June 2010 *Transportation Sector Security Risk Assessment* report that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. For example, the Risk Assessment excluded certain types of threats, such as from lone wolf operators. According to TSA, these limitations will be addressed in the 2011 version.

GAO Contacts

For additional information about this area, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov for overall critical infrastructure protection, or Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov for government facilities.

Appendix VI: Surface Transportation Security

What This Area Includes

Source: TSA.

TSA Rail Security.

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the lead federal agency responsible for overseeing security of all surface transportation modes, which include passenger and freight rail; mass transit; highways, including commercial vehicles; and pipelines. Although TSA has primary responsibility for overseeing surface transportation security, this responsibility is shared with federal, state, and local governments and the private sector. For example, public and private operators are responsible for securing their transportation systems. Key areas within surface transportation security include: (1) risk assessment and planning; (2) standards, inspections, and training; (3) grants; and (4) information sharing. As the primary component responsible for surface transportation security, for fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion for fiscal year 2011, most of which is devoted to aviation security functions. Surface transportation security falls primarily within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are generally focusing on key areas on which we or the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS developed and implemented additional efforts related to surface transportation security on which we are not reporting. These include, among other things, the Surface Transportation Security Priority Assessment—a public-private study which identified recommendations to enhance surface transportation security; the National Explosives Detection Canine Program; the Baseline Assessment for Security Enhancement—a security assessment program designed to evaluate 17 security and emergency management action items for mass transit and passenger rail networks; a training program in Pueblo, Colorado for highway surface transportation inspectors; the Intermodal Security Training and Exercise Program, which is a training and exercise program for the transportation industry developed by TSA, in collaboration with other federal agencies and commercial security vendors; and standard processes for law enforcement to identify and report suspicious incidents or activities throughout the Amtrak rail system and share that information nationally so it can be analyzed to identify broader trends. We have not completed work in these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly TSA, expanded its efforts in key areas on which we have reported, such as risk assessments and strategic planning; surface transportation inspector workforce; grants administration; and information sharing. For example, in 2009 we reported that TSA had begun conducting threat and vulnerability assessments of the commercial vehicle industry and that TSA and other DHS agencies conducted threat, vulnerability, and consequence assessments of highway infrastructure, freight rail, and mass transit. TSA also developed a transportation sector security risk assessment that assessed risk within and across the various transportation modes. In addition, since 2008, TSA more than doubled its surface transportation inspector workforce and reported that, as of July 2011, its surface inspectors conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, among other things. Moreover, we reported in June 2009 that DHS used a risk analysis model to allocate Transit Security Grant Program funding and award grants to higher-risk transit agencies. Further, TSA expanded its sharing of surface transportation security information by establishing information networks.

However, we have identified work remaining in these areas. For example, TSA has strengthened its risk assessments for surface transportation modes, but efforts to further improve elements of these assessments are in the early stages of implementation. Further, TSA has not yet completed an analysis of its surface inspector workforce to direct current and future program needs. Moreover, TSA has not issued regulations for security training programs for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[1] Additionally, we found that TSA should strengthen the management of its program for providing grant funds to transit agencies, and that its information sharing efforts would benefit from improved streamlining and coordination. Table 10 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[1] 6 U.S.C. §§ 1137, 1167, 1184.

Table 10: Assessment of Progress and Work Remaining in Key Surface Transportation Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS employed a strategic approach, including developing national strategies and conducting risk assessments, for each mode of surface transportation, but had not yet developed performance measures for assessing programs' effectiveness.	**DHS developed national strategies for each mode of surface transportation, but had not yet developed measures for assessing progress made in securing surface transportation modes.** **Key progress:** DHS has taken steps to develop and adopt a strategic approach for implementing surface transportation security functions, such as developing national strategies for each surface transportation mode. For example, we reported in June 2009 that TSA's mass transit security strategy contained information related to purpose, scope, and methodology; organizational roles, responsibilities, and coordination; and implementation of the strategy and integration with other strategies. We reported in April 2009 that TSA's freight rail security strategy contained sectorwide goals, subordinate objectives, and performance measures. **What remains to be done:** We identified work remaining in DHS's strategic approaches to security within the different modes of surface transportation. For example, in January 2009, we reported that TSA's highway strategy did not include performance goals and measures with which to assess the program's overall progress toward securing highway infrastructure. In June 2009, we reported that TSA's mass transit security strategy identified sectorwide goals, but did not contain measures or targets for program effectiveness. In August 2010, we reported that TSA's pipeline security strategy identified goals and objectives, but did not include performance measures or milestones. Also, in April 2009, we reported that TSA's freight rail security strategy could be strengthened by including targets for three of its four performance measures and revising its approach for the other measure, such as including more reliable baseline data to improve consistency in quantifying results. We recommended that TSA strengthen its performance measures in its strategies by, for example, measuring the agency's performance in achieving the goals of preventing and deterring acts of terrorism and enhancing the resiliency of mass transit systems. DHS concurred with our recommendations and reported that it was incorporating a risk-based approach with measurable baselines in its updated highway strategy, and revising its mass transit security strategy to incorporate elements to improve its ability to measure agency and industry progress toward achieving mass transit and passenger rail security performance goals. DHS provided its updated transportation security strategy to congressional committees in June 2011 and to us in August 2011. As the strategy was recently issued, we have not yet assessed the extent to which it addresses our recommendations.

TSA conducted risk assessments within and across the transportation sector, but efforts to strengthen these assessments in certain areas are in the early stages of implementation.

Key progress: TSA conducted risk assessments across the transportation sector and for individual transportation modes. In March 2009, we reported that TSA implemented certain aspects of the *National Infrastructure Protection Plan's* risk management framework, such as developing security goals and a database to track assets and systems. In February 2009, we reported that TSA began conducting threat and vulnerability assessments of the commercial vehicle industry. In January, April, and June 2009, we reported that TSA and other DHS agencies took actions to conduct threat, vulnerability, and consequence assessments of highway infrastructure, freight rail, and mass transit and passenger rail, respectively. Further, in August 2010, we reported that TSA developed a pipeline risk assessment model that combined threat, vulnerability, and consequence to create a risk score for each of the 100 most critical pipeline systems in the United States.

What remains to be done: We identified weaknesses in DHS's risk assessments, which TSA has worked to address. For example, we reported in March 2009 that TSA had not conducted comprehensive risk assessments that integrate threat, vulnerability, and consequence for each mode or the transportation sector. We also reported that TSA should strengthen its internal controls to help implement the *National Infrastructure Protection Plan*'s risk management framework, and that TSA did not assign uncertainty or confidence levels to the intelligence information the agency used to identify threats and guide long-range planning and strategic investment. Additionally, in January 2009 we reported that federal entities—including component agencies and offices within DHS and the Department of Transportation—were not systematically coordinating their efforts to assess highway infrastructure risk or sharing the results of those efforts. In April 2009, we reported that TSA's efforts to assess risk to freight rail primarily focused on rail shipments of certain highly toxic materials, although other federal and industry assessments had identified additional potential security threats, including risks to bridges and tunnels. Additionally, as we reported in August 2010, a pipeline system's risk ranking was not TSA's primary consideration in scheduling Corporate Security Reviews—assessments of pipeline operators' security planning—of pipeline operators or Critical Facility Inspections of pipeline systems.

		We recommended strengthening risk assessments across surface transportation modes. DHS generally concurred and in June 2010 TSA produced the Transportation Sector Security Risk Assessment, which assessed risk within and across the various aviation and surface transportation modes, and incorporated threat, vulnerability, and consequence. However, TSA noted limitations—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. In June 2011, agency officials stated that TSA is addressing these limitations in the next version, which is scheduled for completion by the end of 2011. TSA also established an Executive Risk Steering Committee, which, according to TSA officials, serves as a focal point for strategic risk management. Further, in February 2010, TSA officials stated that the agency had met with other federal agencies that conduct security reviews of highway structures to identify existing data resources, establish a data-sharing system among key agencies, and discuss standards for future assessments. In July 2011, TSA further reported that in 2010 it worked with federal partners to conduct comprehensive structural security assessments of 30 highway structures, such as bridges, tunnels, and terminals. This effort is still in the early stages, with the first report of results under review by TSA and its federal partners. In August 2011, TSA officials stated that the first report for highway bridge and tunnel assessments is expected to be complete before the end of calendar year 2011, and with more to be concluded for presentation to stakeholders by the end of calendar year 2012. As DHS has not yet reported on these assessments, it is too early to review their results. Moreover, TSA is developing a Critical Infrastructure Risk Tool to measure the criticality and vulnerability of freight railroad bridges and tunnels. As of July 2011, TSA officials stated that they had begun working with industry officials to raise awareness of cyber risks to the rail system, although TSA has not conducted assessments of those risks. In addition, in June 2011, TSA reported that it had revised its Corporate Security Review Program's standard operating procedure to identify that the primary selection criterion for scheduling Corporate Security Reviews will be the measure of relative risk, although other factors and considerations will also play a role. While these are positive actions, as TSA is in the process of implementing them, it is too early to assess their effectiveness.
Standards, inspections, and training	DHS more than doubled its surface transportation inspector workforce, but has not issued regulations for security training programs for some surface transportation employees.	**TSA deployed an inspector workforce for surface transportation security, but has not issued regulations for security training programs for mass transit, rail, and bus employees.** **Key progress:** We reported in April 2010 that since 2008 TSA more than doubled its surface transportation inspector workforce, and expanded the roles and responsibilities of surface inspectors to include participation in Visible Intermodal Prevention and Response teams, among other things.[a] TSA reported that, as of July 2011, TSA's surface inspectors conducted security assessments of 193 mass transit and passenger rail agencies, and had conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, which gather detailed information on a station's physical security elements, geography, and emergency points of contact.[b]

What remains to be done: In June 2009, we reported that TSA had not completed an analysis of its surface transportation inspector workforce to direct current and future program needs. In March 2010, TSA completed a workforce study that was designed to provide the agency with a more reasonable basis for determining the optimal workforce size needed to achieve its current and future inspector workload needs. However, TSA's workforce study was not specific to surface transportation security inspectors, and we have not assessed the extent to which the results of this study are informing TSA's resource allocation decisions. In addition, the authors of the study suggested using their report as a first step toward further study and a more comprehensive and well-coordinated TSA-wide plan of action. TSA also developed a detailed work plan for inspectors—including surface inspectors—for fiscal year 2011. However, neither the work plan nor the workforce study addresses future hiring and training needs for the surface inspector workforce. In August 2011, TSA officials stated that it would be difficult to make such long-term plans until certain key surface transportation rules have been finalized, such as those for security training discussed in the next section, because these rules will directly affect the surface transportation inspector workload.

Additionally, we identified gaps in DHS's efforts to implement surface transportation security training requirements. In June 2009, we reported that TSA had not 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.[c] We recommended that DHS develop a plan with milestones for implementing provisions of the Act. DHS concurred and in June 2011 stated that it had developed a timeline for completing requirements of the Act, to include issuing the training regulations. TSA reported in July 2011 that it is finalizing the proposed security training program regulations and expects to issue a Notice of Proposed Rulemaking for public comment by January 2012.[d] As DHS is in the process of developing these security training program regulations, it is too soon to assess the extent to their effectiveness. As we reported, the implementation of these regulations will be part of a fundamental shift in approach for TSA as it assumes more of a regulatory role in securing mass transit and passenger rail.

Grants	DHS allocates transit grant funding based on risk assessments and has taken steps to measure performance of the Transit Security Grant Program.[e] However, TSA should further strengthen its management of the grant program.	**DHS implemented the Transit Security Grant Program and uses risk assessments to allocate transit grant funds, but should further strengthen its grants management.** **Key progress:** In fiscal year 2011, DHS made available over $200 million for the Transit Security Grant Program, almost $20 million for intercity rail security, $10 million for freight rail security, and nearly $5 million for intercity bus security. We reported in June 2009 that DHS used a risk analysis model to allocate Transit Security Grant Program funding and award grants to higher-risk transit agencies. The Transit Security Grant Program risk model includes all three elements of risk—threat, vulnerability, and consequence. In addition, DHS developed measures to assess the effectiveness of its grant programs. For example, as the DHS IG reported in December 2010, the Federal Emergency Management Agency (FEMA), in its May 2009 Recovery Act Plan for the Transit Security Grant Program, identified five key performance indicators that it would use to measure the effectiveness of grant performance. Since then, FEMA, working in collaboration with TSA, identified nine additional performance measures for use in conjunction with the measures identified in the May 2009 report. Additionally, TSA reported that it is working with FEMA to develop more robust performance measures to track Transit Security Grant Program management and effectiveness results. FEMA plans to incorporate these performance measures into its fiscal year 2012 grant guidance. In July 2011, TSA also reported a new approach for the Transit Security Grant Program, which focuses resources on the highest risk "shovel ready" transit infrastructure projects, while prioritizing operational deterrence activities such as training and canine teams. **What remains to be done:** We and the DHS IG identified weaknesses in DHS's Transit Security Grant Program, which DHS has worked to address. For example, as we reported in June 2009, in DHS's risk assessments, DHS held vulnerability constant, which limited the model's overall ability to assess risk and DHS's ability to more precisely allocate funds. Moreover, the DHS IG reported in December 2010 that, while DHS developed new performance measures to evaluate the effectiveness of the Transit Security Grant Program, it had not yet implemented a system to collect performance information or to report performance results. Additionally, we reported that the two agencies that manage the Transit Security Grant Program—TSA and FEMA—lacked defined roles and responsibilities, as there was no memorandum of understanding or similar document articulating the roles and responsibilities of the agencies. In June 2011, the DHS IG also reported that TSA did not require Amtrak to develop a corrective action plan addressing the highest ranked vulnerabilities, and TSA approved Amtrak investment justifications for lower risk vulnerabilities.

		Among other things, we and the DHS IG made various recommendations, including that DHS strengthen its methodology for determining risk; incorporate systems to collect information necessary to measure the effectiveness of the Transit Security Grant Program; define TSA's and FEMA's respective roles and responsibilities for managing the Transit Security Grant Program in a memorandum of understanding or similar document; and work closely with Amtrak to establish a corrective action plan and internal procedures that ensure decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by risk assessments. DHS concurred and took steps to address them. For example, TSA and FEMA signed a memorandum of understanding defining roles and responsibilities in March 2011. TSA also reported in July 2011 that the performance measures it developed have been incorporated into FEMA's electronic grant monitoring database and that collection of this data began with the fiscal year 2010 monitoring visits. TSA also reported updating its risk model for the grant program for fiscal year 2012 to better address vulnerability. Additionally, TSA is engaged with Amtrak to develop a comprehensive security plan. As these efforts are underway, it is too early to assess their effectiveness. We have ongoing work assessing DHS's homeland security grant programs, including the Transit Security Grant Program, and plan to report on the results of this work later this year.[f]
Information sharing	DHS expanded its efforts to share surface transportation security information by establishing information networks. However, TSA should better streamline information within and across these networks to avoid duplication as well as improve awareness of key mechanisms, and measure program effectiveness.	**DHS took steps to share surface transportation security information with stakeholders in different sectors, but should do more to streamline information-sharing mechanisms to reduce overlap, improve awareness of certain key mechanisms, and measure program effectiveness.** **Key progress:** DHS established the Homeland Security Information Network, a secure Web site that serves as a clearinghouse of information on available security technologies that have been tested and evaluated by DHS, in addition to providing security alerts, advisories, and information bulletins. Within the Homeland Security Information Network, each of the 18 critical infrastructure sectors maintains its own site, and under the transportation sector, there are sites for different transportation modes. We reported in September 2010, that 75 percent of the public transit agencies we surveyed reported being generally satisfied with the security-related information they received. Preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate general satisfaction among aviation, rail, and highway stakeholders.[g]

	What remains to be done: We have identified challenges to DHS's surface transportation security information sharing efforts. For example, we reported in September 2010 that some public transit agencies cited the need for more streamlined information, and we identified the potential for overlap between three federal information-sharing mechanisms: the Public Transportation Information Sharing and Analysis Center,[h] the Public Transit Portal on the Homeland Security Information Network, and TSA's Office of Intelligence's page on the Homeland Security Information Network,[i] which all receive federal funding and communicate similar unclassified and security-related information to public transit agencies. We also reported that less than half of public transit agencies responding to our survey reported that they had log-in access to the Homeland Security Information Network and had not lost or forgotten their log-in information. Our survey also identified that 12 of the 19 transit agencies that did not have access to the network had never heard of it. An additional 11 agencies did not know whether they had access. Preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate a similar lack of access or awareness among aviation, rail, and highway stakeholders. Preliminary observations also indicate that some freight rail stakeholders would prefer to receive more analysis or actionable information from TSA that could help predict how certain events may affect rail systems. In addition, DHS and TSA have not developed performance goals and outcome-oriented measures to gauge the results of activities for the mechanisms established as primary information sources for the public transportation industry. We recommended that DHS establish time frames for a working group of federal and industry officials to assess opportunities to streamline information-sharing mechanisms to reduce any unneeded overlap and conduct targeted outreach efforts to increase awareness of the Homeland Security Information Network among agencies that are not currently using or aware of this system. We also recommended that DHS develop goals and related outcome-oriented performance measures specific to each of the three security information networks. DHS concurred, and took steps to help address the recommendations. For example, TSA and key industry groups developed a report and associated library, which is intended to streamline the analysis, sharing, and exchange of intelligence and security information that had been disseminated by multiple sources.[j] However, as we reported in June 2011, the report may reduce the number of security-related emails that public transit agencies receive, but it does not reduce overlap among the three information-sharing mechanisms. TSA officials stated that they are continuing to coordinate with other members of the working group to identify actions and time frames for addressing our recommendation, including user satisfaction and performance measures. In addition, we are continuing to assess TSA's efforts related to sharing security information with stakeholders in the aviation, rail, and highway modes and will report the final results later this year.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Visible Intermodal Prevention and Response teams employ a variety of tactics to deter terrorism, including random high-visibility patrols at mass transit and passenger rail stations using, among other things, behavior-detection officers, canine detection teams, and explosive-detection technologies.

[b] We did not independently verify the accuracy of these data.

[c] The Implementing Recommendations of the 9/11 Commission Act of 2007 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.

[d] TSA also reported that it has distributed training products to employees in surface modes, such as a self-study training program for freight rail employees on the recognition and identification of improvised explosive devices.

[e] The Transit Security Grant Program is one of six grant programs that constitute DHS's transportation security grant portfolio. The Transit Security Grant Program provides funds to owners and operators of mass transit and passenger rail systems (which include intracity bus, commuter bus, and all forms of passenger rail, including Amtrak) to protect critical surface transportation infrastructure.

[f] We are completing this work at the request of the House Committee on Homeland Security; the Senate Committee on Homeland Security and Governmental Affairs; and the Senate Committee on Commerce, Science, and Transportation.

[g] This work is being conducted in response to a mandate in the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-35 (2007). We plan to issue our findings on this work later this year.

[h] The Public Transportation Information Sharing and Analysis Center, which is implemented by the American Public Transportation Association and funded by TSA, collects, analyzes, and distributes security and threat information from the federal government and open sources on a 24/7 basis.

[i] TSA's Office of Intelligence implemented its page on the Homeland Security Information Network in March 2010 as a collaborative information-sharing platform for all transportation modes, including public transit.

[j] The Transit and Rail Intelligence Awareness Daily report includes a daily publication to enhance situational awareness, an alert message to provide immediate awareness of a developing threat or incident, and a catalogue of supporting reports and related documents.

GAO Contact

For additional information about this area, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

Appendix VII: Border Security

What This Area Includes

Source: CBP.

Border Patrol Agents.

Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is the lead agency responsible for implementing the department's border security mission. Key areas include

- inspecting travelers at ports of entry;[1]
- inspecting cargo and goods at ports of entry while facilitating commerce;
- securing the border between ports of entry, for example, to reduce illegal immigration through the use of fencing and technology;
- enhancing visa adjudication security and preventing travel document fraud; and[2]
- collaborating with other stakeholders on border security efforts.

As the primary component responsible for border security, for fiscal year 2011, CBP had approximately 61,000 personnel and its budget authority was about $11.3 billion. Border security primarily falls within the Quadrennial Homeland Security Review Mission 2: Securing and Managing our Borders.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to border security also include managing border security resources, such as facilities, assets and human capital, we are not reporting on DHS's progress and work remaining in these areas. DHS also has other border security efforts underway on which we are not reporting. For example, CBP developed and implemented a number of border security programs and efforts to, among other things, address threats posed by the illicit narcotics trade, and acquire or develop new technologies for the southern and northern borders—such as detection sensors to detect illicit tunnels at the southern border. CBP also developed new border security strategies with Canada and Mexico. Other specific programs implemented by CBP include the Immigration Advisory

[1] Ports of entry are government-designated locations where CBP inspects persons and goods to determine, for example, whether they may lawfully enter the country. A land port of entry may have more than one border crossing point where CBP inspects travelers for admissibility into the United States.

[2] Within DHS, U.S. Immigration and Customs Enforcement (ICE) is the lead agency responsible for efforts related to enhancing visa adjudication security.

Program, in which CBP officers are posted at foreign airports and work with host countries' border security agencies and airlines to identify potentially inadmissible aliens, including those who may have ties to terrorism, prior to boarding commercial aircraft to the United States; and the National Targeting Center and the Automated Targeting System for identifying high-risk travelers and cargo.[3] We have not completed recent work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS has expanded its efforts in key border security areas, such as inspection of travelers, cargo, and goods at ports of entry; security of the border between ports of entry; visa adjudication and travel document security; and collaboration with other border security stakeholders. For example, our work has shown that DHS has undertaken efforts to keep terrorists and other dangerous people from entering the country, and from October 1, 2010, through June 30, 2011, CBP reported encountering over 164,000 individuals at ports of entry who were found to be inadmissible into the United States. In addition, checkpoints generally located 25 to 100 miles from the border have contributed to DHS's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. According to Border Patrol data, checkpoint operations accounted for over one-third of the Border Patrol's total drug seizures. However, our work and that of the IG have shown that key challenges remain in these efforts. For example, addressing weaknesses in port of entry traveler inspection procedures and infrastructure would increase assurance that dangerous people and illegal goods would be interdicted at the border. DHS has also not yet decided how to implement a biometric system for recording foreign nationals' exit from the United States. 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 (SBI*net*)—which DHS canceled. 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

[3] The National Targeting Center vets passenger and crew manifests against information available to it to identify, for example, high-risk travelers, and identifies high-risk shipments for inspection. The Automated Targeting System is a computerized model used for targeting cargo for inspection.

transitioning to a new approach for border technology, which we are assessing. DHS also should establish performance measures or management controls for key border security programs. Table 11 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 11: Assessment of Progress and Work Remaining in Key Border Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Inspection of travelers at ports of entry	CBP facilitated cross-border movement of millions of travelers while also working to keep terrorists and dangerous people from entering the country through use of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), its officer training programs, and other programs. However, weaknesses exist in traveler inspection procedures and infrastructure, and DHS does not yet have an integrated approach for tracking foreign nationals' exit from the United States.	**CBP took actions to keep terrorists and dangerous foreign nationals from entering the country at ports of entry while also facilitating the cross-border movement of millions of travelers through the use of the US-VISIT program and its officer training programs, but addressing weaknesses in these and other programs would increase assurance that dangerous people and illegal goods would be interdicted at the border.** **Key progress:** From October 1, 2010 through July 30, 2011, CBP reported encountering about 164,000 individuals at ports of entry who were found to be inadmissible into the United States, and transferred custody of more than 6,100 people with active warrants for other law enforcement purposes.[a] DHS has also undertaken an effort—the US-VISIT program— in order to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information. The entry capability has operated since 2006 at about 300 air, sea, and land ports of entry and, in November 2009, we reported that DHS had established integrated project management plans for, and had begun to interact with and involve stakeholders in, developing an exit capability. DHS reports that, through fiscal year 2011, it has been appropriated about $3.2 billion for US-VISIT.[b] As of July 2011, program officials reported that about $193 million of the appropriation had been obligated to develop air/sea and land exit solutions since 2002.[c] Further, we have work underway examining CBP's training program for CBP officers who conduct inspections at ports of entry.[d] Our preliminary observations indicate that CBP followed federal training guidelines as well as training development best practices in revising its training program for newly hired officers. In doing so, CBP addressed a previous recommendation we made that it strengthen the on-the-job portion of its training program for these newly hired officers. **What remains to be done:** We have identified weaknesses in traveler inspections and challenges to fully implementing the US-VISIT program. As we reported, from 2007 through 2011, addressing weaknesses in port of entry traveler inspection procedures and infrastructure, as well as insufficient training for CBP officers, would increase assurance that dangerous foreign nationals and illegal goods could not unlawfully enter the country; and that currency and firearms could not be smuggled out of the country and finance drug trafficking organizations and sponsors of terrorism. Although CBP's goal is to interdict all violators, CBP estimated that several thousand inadmissible aliens and other violators entered the country through ports of entry in fiscal year 2011.

	Moreover, in November 2009, we reported that DHS had not adopted an integrated approach to scheduling, executing, and tracking the work that needed to be accomplished to deliver a comprehensive exit solution as part of the US-VISIT program. We concluded that, without a master schedule that was integrated and derived in accordance with relevant guidance, DHS could not reliably commit to when and how it would deliver a comprehensive exit solution or adequately monitor and manage its progress toward this end. In particular, we reported that the program faced strategic, operational, and technological challenges at land ports of entry.[e] Further, in August 2010 we reported that an exit capability was not yet implemented and that limitations in the scope, approach, and reporting of air exit pilot scenarios for the program restricted the pilots' ability to inform a decision for a long-term air exit solution. To better provide for the successful delivery of a comprehensive US-VISIT exit solution, we recommended that DHS ensure that an integrated master schedule be developed and maintained in accordance with key practices. DHS concurred and reported, as of July 2011, that the documentation of schedule practices and procedures is ongoing, and that an updated schedule standard, management plan, and management process that are compliant with schedule guidelines are under review. DHS officials also reported that although the department operated several pilot biometric exit programs over the years and learned much from evaluations of those efforts, many challenges remain. As such, DHS stated that it continues to examine all options in connection with a final biometric air exit solution, and has recently given consideration to using its authority to establish an advisory committee to study and provide recommendations to DHS and Congress on implementing an air exit program. In addition, preliminary observations from our ongoing work on CBP training has identified management weaknesses in its training program for incumbent officers that may be limiting CBP's ability to identify and provide the necessary training for these officers. We plan on reporting the final results of this work later this year.

Inspection of cargo and goods at ports of entry while facilitating commerce	CBP improved the security and efficiency of the inspection of cargo and goods while facilitating commerce through the deployment of imaging technology and programs such as the Free and Secure Trade program. However, CBP needs to complete its study on data system enhancements.	**Through the deployment of imaging technology and programs such as the Free and Secure Trade program, CBP improved the efficiency of inspection and security of cargo and goods at ports of entry while facilitating commerce, but needs to complete a study on program benefits.** **Key progress:** CBP reported that the deployment of imaging technology at ports of entry to detect individuals hidden within vehicles, contraband, or other smuggled merchandise in vehicles and cargo had resulted in over 1,000 seizures, which included 292,000 pounds of narcotics from October 1, 2010 through June 30, 2011. In March 2011, the DHS IG reported that while CBP has policies and procedures in place, field personnel did not always receipt and record, transport, store, or dispose of seized drugs according to established policies and procedures, and in some cases, circumvented established guidance by using invalid waivers. The DHS IG attributed these conditions to insufficient oversight, communication, and staffing throughout key stages of the seizure process. Among other things, the DHS IG recommended that CBP strengthen communication and oversight to ensure field personnel comply with seizure procedures. In July 2011, DHS reported that it had implemented the recommendation to monitor personnel compliance with policies and procedures for processing drug seizures. Further, DHS officials reported using additional cargo screening measures. For example, CBP reported that it used large-scale X-ray and gamma ray imaging systems to perform examinations of cargo without having to unload cargo for manual searches or examination of conveyances by methods such as drilling or dismantling. In addition, DHS reported that it began screening 100 percent of southbound rail shipments for unlawful smuggling of weapons, drugs, and cash. Further, to facilitate the travel of low-risk screened shipments across the border and expedited border processing, the United States and Canada participate in the Free and Secure Trade program.[f] In July 2010, we reported that CBP officials and stakeholders we interviewed said that wait times for commercial vehicles traveling across the border into the U.S. had generally decreased under this program. **What remains to be done:** In July 2010, we reported that CBP lacked data needed to assess whether participants in the Free and Secure Trade program experienced intended program benefits, such as expedited border processing. Among other things, we recommended that CBP conduct a study to determine if program benefits are being realized. As we reported, such a study would enable CBP to determine if the benefits are experienced by all program participants and what program adjustments, if any, are needed. DHS concurred and reported in July 2011 that once the enhancements to its data systems were complete, it would conduct a study within 120 days to determine whether the program was meeting its intended benefits. DHS estimates completion of this study in October 2011. While these plans are positive, it is too early to assess the results of DHS's effort until the study is completed.

Security of the border between ports of entry	DHS deployed technologies to secure the border between ports of entry and reduce illegal immigration. In addition, checkpoints contributed to Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. However, DHS has experienced schedule delays and significant performance problems with the technology portion of the Secure Border Initiative and should improve its implementation of checkpoints through enhanced design, staffing, and performance measurement.	**DHS deployed technologies to secure the border between ports of entry and reduce illegal immigration, but DHS experienced schedule delays and significant challenges with meeting cost-effectiveness and viability standards for these technologies.** **Key progress:** In November 2005, DHS launched the Secure Border Initiative (SBI), a multiyear, multibillion dollar program aimed at securing U.S. borders and reducing illegal immigration. Through this initiative, DHS planned to develop a comprehensive border protection system using technology, known as SBI*net*, and tactical infrastructure—fencing, roads, and lighting. In March 2011, we reported that surveillance capability deployed through this initiative was being used in Arizona, and that the CBP Office of Border Patrol considered these capabilities to be useful, for example, by providing continuous surveillance in border areas where none existed before. In addition, in May 2010 we reported that CBP had completed deploying most of its planned tactical infrastructure, including 646 of the 652 miles of fencing. **What remains to be done:** Since the inception of SBI, we reported on significant management weaknesses and risks. With regard to tactical infrastructure, we reported in September 2009 that its impact on border security had not been measured and as a result, DHS was not positioned to assess the impact of this investment. Overall, DHS reported achieving an acceptable level of border control across less than half of the southwest border and less than 2 percent of the northern border during fiscal year 2010.[g] Among other things, we recommended that CBP conduct a cost-effective evaluation of the impact of tactical infrastructure. DHS generally concurred and reported actions underway to address this recommendation. For example, in June 2011, CBP stated that analysis initially conducted by the Homeland Security Institute in April 2010 on the impact of tactical infrastructure had been expanded to include other data and information, and that DHS expects to deliver a final report in February 2012.

With regard to SBI*net*, in September 2008 we reported that CBP's plans to initially deploy SBI*net* technology along the southwest border had slipped from the end of 2008 to 2011. In January 2010 we reported that DHS had not effectively managed key aspects of SBI*net* testing and that DHS test plans, cases, and procedures for the test events were not defined in accordance with important elements of relevant guidance. In May 2010, we reported that because of SBI*net*'s decreased scope, uncertain timing, unclear costs relative to benefits, and limited life cycle management discipline and rigor, it was unclear whether the department's pursuit of SBI*net* was a cost effective course of action. Moreover, in October 2010 we reported that DHS needed to strengthen management and oversight of its *SBInet* contractor. Among other things we recommended (1) limiting near-term investment in the first incremental block of SBI*net*,[h] (2) economically justifying any longer-term investment in SBI*net*, and (3) improving key program management disciplines. DHS generally agreed with our recommendations. In January 2011, the Secretary of Homeland Security directed CBP to end the SBI*net* program as originally conceived because it did not meet cost-effectiveness and viability standards, and to instead focus on developing solutions utilizing existing, proven technology, such as camera-based surveillance systems, for each border region. Given that DHS is transitioning to a new approach—the Alternative (Southwest) Border Technology plan—we and DHS are assessing the extent to which the issues we identified with respect to SBI*net* are applicable to the new plan.

The Alternative (Southwest) Border Technology plan is to incorporate a mix of technology, including an Integrated Fixed Tower surveillance system similar to that used in the current SBI*net* capability, beginning with high-risk areas in Arizona. In March 2011, we reported that due to a number of reasons, the cost-effectiveness and operational effectiveness and suitability of the Integrated Fixed Tower system was not yet clear. First, the analysis of alternatives DHS used to inform its decision to cancel SBI*net* cited a range of uncertainties, and it was not clear how the analyses and conclusions were factored into planning and budget decisions regarding the optimal mix of technology deployments in Arizona. Second, independent analyses conducted by the Army's Test and Evaluation Command were not complete at the time of the Secretary's decision to cancel SBI*net*, thus any results on SBI*net*'s operational effectiveness and suitability could not inform the decisions to proceed with the Integrated Fixed Tower system. DHS did not agree with our observations on the analysis of alternatives and the potential usefulness of the Army's Test and Evaluation Command. We believe our observations are valid.

Checkpoints contributed to the Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. However, the need to strengthen checkpoint design and staffing, and improve the measurement and reporting of checkpoint effectiveness has impeded higher levels of performance.

Key progress: CBP's Border Patrol uses checkpoints to protect the nation from the impact of contraband illegally smuggled across the border, and from removable aliens, some of whom may have ties to organized crime or countries at a higher risk of having groups that sponsor terrorism. In August 2009 we reported that checkpoints had contributed to the Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. Moreover, checkpoint operations accounted for over one-third of the Border Patrol's total drug seizures, according to Border Patrol data.

		What remains to be done: In August 2009, we reported on factors that impeded higher levels of performance with regard to checkpoints. For example, Border Patrol officials we spoke with said that additional staff, canine teams, and inspection technology were needed to increase checkpoint effectiveness. In addition, we reported that a lack of management oversight and unclear checkpoint data collection guidance resulted in the overstatement of checkpoint performance results in fiscal year 2007 and 2008 agency performance reports, as well as inconsistent data collection practices at checkpoints. Moreover, Border Patrol was not yet using performance measures it had developed to examine the extent to which checkpoint operations affected quality of life in surrounding communities. We recommended that CBP strengthen checkpoint design and staffing, and improve the measurement and reporting of checkpoint effectiveness, including community impact. Implementing performance measures would serve to provide greater attention and priority in Border Patrol operational and staffing decisions to address any existing issues at checkpoints and strengthen program accountability. CBP concurred and has reported actions underway to address them. For example, in July 2011 CBP reported that it had acquired the services of the DHS Science and Technology Centers of Excellence (University of Arizona and University of Texas, El Paso) to assist in measuring the effectiveness of checkpoints, and to assess the economic and social impacts of permanent checkpoints on the surrounding communities. DHS officials expect a final report on or about the end of fiscal year 2012.
Visa adjudication security and preventing travel document fraud	DHS improved programs designed to enhance visa security, including the Visa Security Program, Visa Waiver Program, and the Western Hemisphere Travel Initiative. However, further steps are needed to evaluate these efforts, address potential risks, and enhance training and oversight.	**DHS contributed to the enhancement of visa adjudication security; however, further steps are needed to evaluate these efforts.** **Key progress:** In March 2011, we reported that the DHS Visa Security Program, which is administered by U.S. Immigration and Customs Enforcement (ICE), is a part of the visa screening process at certain embassies and consulates in which ICE personnel review visa applications to help prevent individuals who pose a threat from entering the United States. The Visa Security Program is currently deployed to 19 posts in 15 countries. Moreover, we reported that ICE had developed a 5-year expansion plan in 2007 for the Visa Security Program. In addition, in August 2011, CBP reported that it had implemented a new program for continuously vetting recently issued U.S. nonimmigrant visas for derogatory information that becomes available subsequent to visa issuance. CBP reported that if it uncovers such derogatory information, it alerts the Department of State that the traveler may no longer be eligible for the visa.

What remains to be done: In March 2011, we reported that ICE needed to improve performance evaluation of the Visa Security Program and better address visa risk worldwide. Specifically, we reported that ICE could not accurately assess progress toward its program objectives because, among other things, the tracking system it used to collect data on program activities did not gather comprehensive data on all the performance measures needed to evaluate mission objectives. Moreover, we reported that ICE did not fully follow or update its 5-year expansion plan. For instance, ICE 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. We made recommendations designed to address these weaknesses. DHS concurred with some of these recommendations, and stated that it is taking steps to address them. For example, DHS stated that it is identifying alternatives for Visa Security Program review at high risk posts that do not have a physical Visa Security Program presence. DHS did not concur with other recommendations, including that the program collect comprehensive data on all performance measures and track the time spent on visa security activities. DHS stated that the Visa Security Program captured all of the required performance metrics identified in its 5-year expansion plan. However, we reported that while ICE was collecting some data on the performance measures identified in its plan, our analysis showed that the data were not sufficient to accurately demonstrate the progress made toward achieving program objectives.

DHS has taken steps intended to enhance the security of the Visa Waiver Program, which enables eligible citizens of participating countries to travel to the United States without first obtaining a visa, but has not yet fully evaluated and addressed program risks.

Key progress: In May 2011, we reported that DHS had implemented an electronic authorization system for screening and determining the eligibility of potential visa waiver travelers in advance of their travel—the Electronic System for Travel Authorization. In May 2011, we reported that DHS requires that Visa Waiver Program countries enter into information-sharing agreements with the United States; however, only half of the countries fully complied with this requirement and many of the signed agreements had not been implemented. Half of the countries had entered into agreements to share watchlist information about known or suspected terrorists and to provide access to biographical, biometric, and criminal history data. Almost all of the 36 Visa Waver Program countries had entered into an agreement to report lost and stolen passports. DHS, with the support of interagency partners, had established a compliance schedule requiring the last of the Visa Waver Program countries to finalize these agreements by June 2012.

What remains to be done: In May 2011, we reported that DHS had not fully evaluated security risks related to the small percentage of Visa Waiver Program travelers without verified approval by the system to know to what extent they posed a risk to the program.[i] Moreover, we reported that DHS had not completed 18 of the 36 most recent required reports on Visa Waiver Program countries' security risks in a timely manner, and as result, it was unclear whether vulnerabilities existed that jeopardized continued participation in the Visa Waiver Program.[j] We recommended that DHS establish time frames for the regular review of cases of Electronic System for Travel Authorization noncompliance and address delays in the biennial country review process to ensure timely completion. DHS concurred with our recommendations, and in July 2011 DHS stated that it established procedures to perform quarterly reviews of a representative sample of Visa Waiver Program passengers who do not comply with the Electronic System for Travel Authorization requirement to determine the level of risk posed to Visa Waiver Program security and identify improvements to minimize noncompliance. While these are positive steps, as DHS has just taken these actions, it is too early to assess their impact.

DHS improved the Western Hemisphere Travel Initiative, but this initiative would be strengthened by enhanced training, oversight, and guidance.

Key progress: The Western Hemisphere Travel Initiative required, as of June 1, 2009, for land and sea travel and as of January 23, 2007, for air travel, certain travelers who previously were allowed to enter the United States from within the Western Hemisphere without passports to present passports or other approved documents to enter the United States.[k] According to DHS, the Western Hemisphere Travel Initiative improved CBP's ability to identify individuals misrepresenting themselves or falsely claiming U.S. citizenship. In February 2011, the DHS IG reported that CBP successfully implemented these requirements in the air environment, and because the requirements improved CBP officers' ability to validate the identity and citizenship of compliant air passengers, officers were able to spend more time inspecting travelers without passports. In addition, CBP reported the average inspection process time as having been reduced since implementation of the Western Hemisphere Travel Initiative and that this initiative has promoted more efficient processing of travelers into the United States.

What remains to be done: The DHS IG reported that, due to inadequate incumbent officer training, oversight, and guidance, there was insufficient assurance that CBP officers verified the identity and citizenship of all individuals who did not provide a passport or other compliant documentation. In addition, the DHS IG recommended, among other things, that CBP implement procedures for monitoring CBP officers' compliance with Western Hemisphere Travel Initiative enforcement procedures. DHS concurred and identified actions to implement procedures for monitoring compliance. For example, in July 2011 CBP reported that it plans to clarify and reissue guidance and provide refresher training to CBP officers on Western Hemisphere Travel Initiative compliance and procedures for noncompliant travelers by September 2011. In addition, CBP reported that it planned to implement procedures for monitoring CBP officers' compliance with CBP policy regarding the Western Hemisphere Travel Initiative enforcement procedure using CBP's Self Inspection Program by December 2011.

Collaborating on border security efforts	DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts through interagency forums and joint operations. However, DHS should strengthen cooperation through enhanced oversight to ensure efficient use of interagency forums and improved information sharing.	**DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts such as interagency forums, but should strengthen cooperation through better oversight of these forums and information sharing.** **Key progress:** In December 2010 we reported that federal, state, local, tribal, and international law enforcement partners reported improved DHS coordination to secure the northern border. For example, interagency forums helped in establishing a common understanding of border security threats, while joint operations helped to achieve an integrated and effective law enforcement response. **What remains to be done:** We found that more work remains in sharing information and resources useful for operations for northern border security. For example, partners in all four sectors we visited cited ongoing challenges sharing information and resources for daily border security, and that oversight by management at the component and local level has not ensured consistent compliance with provisions of interagency agreements, such as those related to information sharing. Among other things, we recommended that DHS enhance oversight to ensure the efficient use of interagency forums and compliance with interagency agreements. DHS concurred and has taken steps to address the recommendations, such as reviewing the inventory of interagency forums through its strategic and operational planning efforts to assess efficiency and identify challenges. DHS officials reported in July 2011 that the department plans to release a strategy that will articulate a department-level approach to more efficiently and effectively secure and manage the U.S. northern border. Officials reported that this overarching framework will emphasize intra-DHS coordination as well as enhanced collaboration with federal, state, local, tribal, territorial and Canadian partners. The department is still determining the best path forward for implementing the goals of the strategy, and stated that any implementation effort will require enhanced coordination between DHS components, including CBP Office of Border Patrol and ICE, as well as improved cooperation with partners on both sides of the border.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] CBP's Office of Field Operations reported that of the total individuals at ports of entry who were found to be inadmissible into the United States, 55,903 were at the southern land border and 24,066 were at the northern land border. The remaining inadmissible individuals were at sea ports (52,366), air ports (29,049), and other uncategorized inadmissible events (2,818). We did not independently verify the accuracy of these data.

[b] DHS was appropriated about $335 million for US-VISIT for fiscal year 2011. Pub. L. No. 112-10, § 1629, 125 Stat. 38, 143 (2011).

[c] We did not independently verify the accuracy of these data.

[d] We are conducting this work for the House Committee on Homeland Security.

[e] GAO, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248, Washington, D.C.: Dec. 6, 2006.

[f] The United States and Mexico also participate in the Free and Secure Trade program, but the focus of our report was on United States and Canada participation. CBP launched the Free and Secure Trade program in 2002 to expedite processing for pre-vetted, low-risk shipments. The program is intended to secure and facilitate legitimate trade by providing expedited processing of participants' merchandise in designated traffic lanes at select border sites, result in fewer referrals to secondary inspections, enable "front-of-the-line" processing in secondary CBP inspections, and provide for enhanced security.

[g] According to Border Patrol, an acceptable level of border control is established when it has the capability (i.e., resources) to deter or detect and apprehend incursions at the immediate border or after entry.

[h] SBI*net* was being acquired and deployed in incremental blocks of capability, with the first block to cost about $1.3 billion.

[i] Specifically, we reported that in 2010, airlines complied with the requirement to verify Electronic System for Travel Authorization approval for almost 98 percent of Visa Waiver Program passengers prior to boarding, but the remaining 2 percent—about 364,000 travelers—traveled under the Visa Waiver Program without verified Electronic System for Travel Authorization approval.

[j] The Enhanced Border Security and Visa Entry Reform Act of 2002 increased the frequency—from once every 5 years to at least once every 2 years—of mandated assessments of the effect of each country's continued participation in the Visa Waiver Program on the security, law enforcement, and immigration interests of the United States. The law also directs DHS to determine, based on the evaluation, whether each Visa Waiver Program country's designation should continue or be terminated and to submit a written report on that determination to select congressional committees. 8 U.S.C. § 1187(c)(5)(A)(i).

[k] In July 2008, the Department of State began issuing passport cards as a lower-cost alternative to passports for U.S. citizens to meet Western Hemisphere Travel Initiative requirements. In October 2008, the Department of State began issuing the second generation border crossing card based on the architecture of the passport card. In June 2010 we reported that improvements in the Department of State's development process could increase the security of these documents. See GAO, *Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards*, GAO-10-589, Washington, D.C.: June 1, 2010.

GAO Contact

For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

Appendix VIII: Maritime Security

What This Area Includes

Source: U.S. Coast Guard.

Port of Los Angeles.

Within the Department of Homeland Security (DHS), the U.S. Coast Guard has primary responsibility for maritime security, while various component agencies also contribute to maritime security efforts, including U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and the Domestic Nuclear Detection Office (DNDO).[1] Key areas within maritime security include (1) port facility and vessel security; (2) maritime domain awareness and information sharing; and (3) international supply chain security. The Coast Guard is responsible for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, among other things, it conducts port facility inspections, leads the coordination of maritime information sharing efforts, and promotes domain awareness in the maritime environment. CBP is responsible for the maritime screening of incoming commercial cargo for the presence of contraband, such as explosives, while facilitating the flow of legitimate trade, cargo, and passengers. TSA and the Coast Guard have responsibility for the implementation and enforcement, respectively, of the Transportation Worker Identification Credential program to manage the access of maritime workers to regulated maritime facilities. DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including portal monitors. As one of the primary components responsible for maritime security protection, for fiscal year 2011 the Coast Guard had about 50,000 personnel, including civilian and military, and its budget authority was about $10.2 billion.[2] Maritime

[1] U.S. Immigration and Customs Enforcement (ICE) also contributes to maritime security in that its mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks. In this capacity, ICE contributes to DHS border security efforts, including in the maritime environment, even though its main focus is not interdicting or screening operations.

[2] The budget and personnel figures for Coast Guard include its nonhomeland security related programs, such as its search and rescue mission function. In addition to Coast Guard resources, for fiscal year 2011 CBP had about 61,000 personnel and budget authority of about $11.4 billion; TSA had about 55,000 personnel and budget authority of about $7.7 billion; and the DNDO had about 130 personnel and budget authority of about $340 million. However, the figures for these components include their nonmaritime security related programs for fiscal year 2011.

security primarily falls within the Quadrennial Homeland Security Review Mission 2: Securing and Managing our Borders.[3]

For the purposes of this report, we are generally focusing on key areas on which we and the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to maritime security also include maritime security national planning, we are not discussing DHS's progress and work remaining in this area. DHS has developed and implemented other efforts related to maritime security. For example, according to the Coast Guard, its maritime security programs are part of a layered strategy that begins far from our ports. Coast Guard officials noted that their security regime includes close coordination with international and regional organizations (such as the International Maritime Organization and the European Union), and individual country's coast guard equivalent agencies; security inspections of, and technical assistance to, foreign ports; and maintaining a multi-mission fleet of cutters patrolling our coastal approaches. The Coast Guard also noted that some of its other missions—those not directly part of its ports, waterways, and coastal security mission—can contribute to homeland security.

Further, in July 2011, the Coast Guard reported that it had specific initiatives underway to enhance maritime security planning at the port level, on which we have not previously reported. Specifically, Coast Guard reported that it had updated 43 port-level Area Maritime Security Plans that covered prevention, protection, security response, and short-term recovery, and that these plans were approved by Coast Guard district and area commanders. The Coast Guard further reported that it was working closely with maritime committees and stakeholders to maintain and annually exercise these port-level plans. We have not completed work on these areas upon which to make an assessment.

[3] While Coast Guard's maritime security efforts reported by us and the DHS IG primarily fall within Mission 2 of the Quadrennial Homeland Security Review, according to Coast Guard, its port level maritime security planning efforts fall within Mission 1: Preventing Terrorism and Enhancing Security and Mission 5: Ensuring Resilience to Disasters. For the purposes of this report, we discussed Coast Guard's port level security planning efforts under the maritime security functional area aligned under QHSR Mission 2, as discussed in appendix II on our scope and methodology.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS's components, particularly the Coast Guard and CBP, have expanded their efforts in key areas, such as port facility and vessel security; maritime domain awareness and information sharing; and international supply chain security. The Coast Guard strengthened risk management through the development of a risk assessment model, and developed a strategy and programs intended to address risks to maritime facilities and passenger and commodity vessels. In addition, the Coast Guard increased maritime domain awareness through interagency operational centers, implementing a vessel tracking system, and identifying awareness gaps in the Arctic.[4] For example, in July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements resulting in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness. Further, in July 2011 DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments.

However, our work and that of the DHS IG has shown that more work remains. For example, DHS components' efforts to assess the effectiveness of programs to secure maritime facilities should be improved. We found that because of a lack of technology capability, DHS does not electronically verify identity and immigration status of foreign seafarers as part of its admissibility inspection process, thus limiting the assurance that fraud could be identified among documents presented by them. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, DHS and its partners should enhance efforts to improve maritime domain awareness by, for example, further strengthening tracking of small vessels. In addition, although DHS developed the Transportation Worker Identification Credential program, we found that the program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the

[4] Interagency operational centers are one element of maritime domain awareness, for which other agencies, particularly the Department of Defense, also have responsibilities.

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. Table 12 provides more detailed information on our assessment of DHS's progress and work remaining in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 12: Assessment of Progress and Work Remaining in Key Maritime Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Port facility and vessel security	The Coast Guard strengthened security of port facilities and vessels by developing a risk assessment model; conducting annual inspections; working to prevent unauthorized entry of individuals; and providing additional efforts to secure passenger and commodity vessels. However, the information system for tracking inspections and efforts to assess the effectiveness of security measures should be improved.	**The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. However, difficulties in calculating effects may challenge its ability to conduct risk assessments.** **Key progress:** The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. In July 2010 we noted that the Coast Guard made progress assessing risks by developing the Maritime Security Risk Analysis Model, which is used to assess risk to individual assets and facilities within ports. It is used by each Coast Guard sector, and assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios. The Coast Guard is starting to integrate the results of its risk assessment efforts into resource allocation decisions, including informing decisions about deployment of local assets. Additionally, the Coast Guard is starting to use the Maritime Security Risk Analysis Model results for evaluating capabilities needed to combat future terrorist threats and identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that the results of the risk assessments were used to refine the Maritime Security and Response Operations requirements for the number of cruise ship escorts and patrols of cruise ship facilities.[a] In July 2011, the Coast Guard reported that it had worked with DNDO to add radiological and nuclear threats to the Maritime Security Risk Analysis Model scenarios. **What remains to be done:** We are conducting work examining the Maritime Security Risk Analysis Model, as well as reviewing the role that risk plays in the allocation of resources in the Port Security Grant Program.[b] In August 2011, we testified on the use of the Maritime Security Risk Analysis Model to assess offshore energy facilities. We found that the Coast Guard has several limitations in assessing the risks to such facilities. Such limitations involve calculating secondary economic effects and assessing the systematic or network risks of an attack on offshore energy facilities. We plan to report the results from our ongoing work later this year.

Area	Overall assessment	Summary of key progress and work remaining
		DHS addressed risk to port facilities through annual inspections and efforts to prevent unauthorized entry of individuals. However, risks exist in not electronically verifying the identity and immigration status of foreign seafarers onboard cargo vessels. **Key progress:** DHS has addressed risks to port facilities through annual inspections and programs designed to prevent the unauthorized entry of individuals. Federal law requires certain port facilities to have security plans in place.[c] Coast Guard guidance calls for at least one announced annual inspection and at least one unannounced annual spot check to ensure that plans are being followed. In February 2008, we reported that Coast Guard's inspections were identifying and correcting facility deficiencies. For example, the Coast Guard identified deficiencies in about one-third of the facilities inspected from 2004 through 2006, with deficiencies concentrated in certain deficiency categories, such as failing to follow facility security plans for access control. We are currently conducting work examining, among other things, the way in which the Coast Guard assesses risk and ensures security of offshore energy infrastructure.[d] As part of our review, we plan to analyze offshore infrastructure security plans and the Coast Guard's security inspection reports. We plan to report the final results from this effort later this year. In August 2011, we testified that the Coast Guard should strengthen its internal controls to ensure that required risk assessments are done at appropriate offshore infrastructure. Further, DHS took actions to address risks posed by unauthorized individuals with access to U.S. port facilities. Specifically, in January 2011, we reported on actions the Coast Guard and CBP took to address risk posed by foreign seafarers entering U.S. seaports. We found that the agencies were using a layered security strategy for identifying and addressing risks, and that CBP and the Coast Guard were conducting advance-screening, inspections, and enforcement operations. For example, both CBP and the Coast Guard received and screened advance information on commercial vessels scheduled to arrive at U.S. ports, and prepared risk assessments based on the results of the advance-screening of vessel and seafarer information. We also reported that the Coast Guard may conduct armed security boarding of arriving commercial vessels based on various factors, including intelligence it received to examine seafarer passports and visas, among other things, and ensure the submitted crew list is accurate. In addition, we have reviewed DHS's efforts to manage the access of maritime workers to regulated maritime facilities through the Transportation Worker Identification Credential program. For example, in May 2011, we reported that TSA designed processes to facilitate the issuance of credentials to maritime workers.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: With regard to foreign seafarers, in January 2011 we reported that because of a lack of technology capability, DHS did not electronically verify identity and immigration status on board cargo vessels, thus limiting assurance that fraud was identified among documents presented by foreign seafarers seeking admission into the United States. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, we reported that DHS faced challenges in ensuring it had reliable data on illegal entries by foreign seafarers at U.S. seaports. For example, both CBP and the Coast Guard track the frequency of absconder (a seafarer CBP has ordered detained on board a vessel in port, but who departs a vessel without permission) and deserter (a seafarer CBP grants permission to leave a vessel, but who does not return when required) incidents at U.S. seaports, but the records of these incidents varied considerably among the two agencies. As a result, the data DHS used to inform its strategic and tactical plans were of undetermined reliability. We recommended that DHS assess the risks of not electronically verifying foreign seafarers for admissibility, and that CBP and the Coast Guard determine why their data varied and jointly establish a process for sharing and reconciling records of illegal seafarer entries at U.S. seaports. DHS concurred and reported that CBP met with the DHS Screening Coordination Office to determine risks associated with not electronically verifying foreign seafarers for admissibility. Further, in July 2011 DHS reported that CBP and the Coast Guard were working to assess the costs associated with deploying biometric capabilities to the maritime domain. As these efforts are in the early stages, it is too soon to assess their results. Further, given the number of seafarers transiting U.S. ports each year and the continued threats posed by terrorism to the United States, establishing a process for sharing and reconciling information on absconder and deserter incidents could better support Coast Guard's and CBP's efforts to prevent illegal immigration at U.S. seaports. With regard to the Transportation Worker Identification Credential, in May 2011 we reported that program controls were not designed to provide reasonable assurance that only qualified applicants could acquire the 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. Further, DHS had not assessed the program's effectiveness at enhancing security or reducing risk for federally regulated facilities. We recommended, among other things, that DHS assess the program's internal controls to identify needed corrective actions, assess its effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. DHS concurred and stated that it has initiated a review of current Transportation Worker Identification Credential program internal controls with a specific focus on the controls highlighted in our May 2011 report. As DHS is in the early stages of implementing these actions, it is too early to assess their impact. Until such efforts are completed, it will be difficult for DHS to provide reasonable assurance that the program is meeting its goals and that only qualified applicants can acquire the credentials.

Area	Overall assessment	Summary of key progress and work remaining
		The Coast Guard conducted pre-entry security boarding, escorts, and patrols to secure passenger and commodity vessels, but additional actions and further study are needed. **Key progress:** DHS took measures to help secure vessels including cruise ships, ferries, and energy commodity vessels such as tankers. In April and December 2010, we reported that DHS assessed risks to cruise ships and ferries, respectively, and in December 2007 we reported that DHS took action to prevent and be prepared to respond to attacks on energy commodity tankers. We also reported that DHS took measures to better secure these vessels. For example, the Coast Guard provided escorts for cruise ships to help prevent waterside attacks and a security presence on ferries during transit. CBP conducted reviews of passenger and crew data for terrorist connections or criminal ties and helped to ensure that all passengers and crew are cleared for entry into the United States. Further, with regard to energy commodity tanker security, the Coast Guard conducted security activities, such as pre-entry security boardings, escorts, and patrols. **What remains to be done:** DHS made progress in these areas, but additional actions are needed to further enhance security. For example, we reported that CBP had 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. Additionally, Coast Guard records showed that at some ports, a lack of resources hindered some Coast Guard units from meeting their self-imposed requirements for activities, such as escorts and boardings to secure tankers. We recommended, among other things, that CBP conduct a study to determine whether requiring cruise lines to provide automated passenger data to CBP on a systematic basis would benefit homeland security. We also recommended that DHS develop a national resource allocation plan to balance the Coast Guard's security responsibilities to protect energy commodity vessels with its other mission functions. DHS concurred with our recommendations and reported taking steps to address them. In July 2011, CBP reported that it had conducted site surveys at three ports of entry to assess the advantage of having cruise line booking data considered in a national targeting process, and had initiated discussions with a cruise line association on the feasibility of CBP gaining national access to cruise line booking data. Although CBP had originally set a due date of June 30, 2011, for its full evaluation of these issues, CBP reported that it had requested an extension to September 30, 2011, to obtain information from the cruise industry on potential impacts of requiring them to provide passenger data on a systematic basis. In addition, Coast Guard officials stated that they plan to develop a resource allocation plan, starting in April 2012, as part of the implementation of a national strategy, which is being developed for reducing the maritime security risks present in the bulk transportation and transfer of certain dangerous cargo on commodity vessels. In the interim, the Coast Guard has published guidance to clarify the process' timing and scope to ensure full consideration is given to safety and security of the port, the facility, and the energy commodity vessel. We have reported that actions such as these are important to help ensure that the Coast Guard is positioning itself to address threats to passenger and commodity vessels. As CBP and the Coast Guard are in the early stages of implementing these efforts, it is too soon to assess their effectiveness.

Area	Overall assessment	Summary of key progress and work remaining
Maritime domain awareness and information sharing	DHS strengthened maritime domain awareness through efforts such as establishing interagency operations centers, vessel tracking systems, and identifying security gaps in the Arctic. However, these efforts face challenges including budgetary constraints, difficulty tracking smaller and noncommercial vessels, and the need for improved information sharing with key Arctic stakeholders.	**DHS and its partners are working to establish interagency operations centers to improve maritime domain awareness, but these efforts face budgetary constraints and other challenges.** **Key progress:** The Security and Accountability For Every Port Act of 2006 calls for the establishment of interagency operations centers for port security, directing the Secretary of DHS to establish such centers at all high-priority ports no later than 3 years after the act's enactment (enacted October 13, 2006).[e] In October 2007, we reported that Coast Guard was piloting various aspects of future interagency operations centers at its 35 existing command centers and working with multiple interagency partners to further their development. According to the Coast Guard, future interagency operations centers would allow the Coast Guard and its partners to use port surveillance with joint tactical and intelligence information and share these data with port partners working side by side in expanded facilities. In July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements which resulted in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness. **What remains to be done:** In October 2007, we reported that the Coast Guard faced budget constraints in trying to expand its current command centers and include other agencies at the centers. In our ongoing work looking at the continued implementation of Interagency Operations Centers, our preliminary observations indicate that as of August 2011, the Coast Guard has installed its information sharing system at more than 10 Coast Guard sectors.[f] Based on our preliminary observations, we identified concerns about whether the Coast Guard will meet its goals related to the involvement of port partners. We plan to report the final results of our work later this year.
		DHS implemented vessel-tracking systems, but tracking small vessels poses challenges. **Key progress:** At sea or in U.S. coastal areas, inland waterways, and ports, the Coast Guard relies on a diverse array of vessel tracking systems operated by various entities. 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.[g] 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. In addition, in July 2011, DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. Among other things, DHS reported that this system would allow CBP to identify potential high-risk small boats to determine, for example, which needed to be boarded upon arrival.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We identified limitations in the Coast Guard's efforts to track vessels at sea. In March 2009, we reported that the means of tracking vessels at sea are potentially effective, but each has features that could impede its effectiveness. Also, the systems used in U.S. coastal areas, inland waterways, and ports—automatic identification system, radar, and video cameras—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. To help address the small vessel threat, DHS developed a Small Vessel Security Strategy in April 2008, and in January 2011 issued the implementation plan for the strategy. As DHS is in the process of executing its implementation plan, it is too early to assess its effectiveness in enhancing maritime security.
		DHS identified and addressed some information gaps in the Arctic, but efforts would benefit from improved information sharing. **Key progress:** In September 2010, we reported that, according to Coast Guard officials, establishing domain awareness in the Artic would allow the Coast Guard to better understand the risks associated with operating in or monitoring the region, but that the Coast Guard faced obstacles to achieving domain awareness. Specifically, officials stated that establishing domain awareness was inhibited by (1) inadequate Arctic Ocean and weather data, (2) lack of communication infrastructure, (3) limited intelligence information, and (4) lack of a physical presence in the Arctic. The Coast Guard identified Arctic requirements and gaps for the maritime domain while also collecting relevant information from routine operations. For example, in September 2010 we reported that the Coast Guard established temporary operating locations in the Arctic and conducted biweekly Arctic overflights to obtain more information on the Arctic operating environment. In addition, information gathered during the Coast Guard's routine missions, such as ice breaking and search and rescue, informed Coast Guard requirements for operating in the Arctic region.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: The Coast Guard's success in implementing an Arctic plan rests in part on how successfully it communicates with key stakeholders, especially state and local officials, and Alaska Native tribal governments and interest groups. In September 2010 we reported that 9 of the 15 state and local officials we met with wanted more information on the status and results of the Coast Guard's efforts to develop its future Arctic requirements. For example, some state and local officials believed that the agency had already determined its plan for Arctic operations but had not shared it, and one state official reported that his office and others may be willing to invest in infrastructure that could benefit the Coast Guard if and when they know the agency's plans. Coast Guard officials told us that they have been focused on communication with congressional and federal stakeholders and intended to share Arctic plans with other stakeholders once plans are determined. In the interim, some state and local stakeholders reported having limited information that they believe would be useful on the process and progress of the agency's Arctic planning efforts. We recommended that the Coast Guard communicate with key stakeholders on the process and progress of its Arctic planning efforts. DHS concurred and in July 2011 reported it was taking actions to address our recommendation, such as soliciting comments from indigenous populations and the public on the National Ocean Policy and participating on the International Arctic Council, a high-level forum for promoting cooperation, coordination, and interaction among Arctic nations, indigenous communities, and other Arctic stakeholders on Arctic issues.[h] While these are positive steps, it is too early to assess the outcomes of DHS's consultation efforts.
International supply chain security	DHS made progress in deploying container screening technologies and partnered with foreign governments for supply chain security. However, these efforts would be enhanced by the development of measures to assess the performance of new technologies and the completion of a feasibility analysis of implementing the requirement to scan 100 percent of all U.S.-bound cargo containers.	**CBP made progress in deploying new technologies, but development and implementation of these technologies should be improved through performance standards and alignment with operational needs.** **Key progress:** DHS has made progress in developing technologies to improve container security by detecting intrusions and tracking containers and scanning them for contraband, including nuclear material. DHS conducted research and development for four container security technology projects to detect intrusion and track the movement of containers through the supply chain. For example, DHS's Science and Technology Directorate initiated the Container Security Device project to develop the capability to detect container door intrusion. Further, to detect nuclear materials, CBP, in coordination with DNDO, deployed over 1,400 radiation portal monitors at U.S. ports of entry. Most of the radiation portal monitors are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass. These monitors alarm when they detect radiation coming from a package, vehicle, or shipping container. CBP then conducts further inspections at its secondary inspection locations to identify the cause of the alarm and determine whether there is a reason for concern.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported in September 2010 that DHS had not yet developed performance standards for these new technologies because it had not yet demonstrated that they can effectively work in operational environments. Additionally, DNDO began working on the cargo advanced automated radiography system with the intention that this technology could be used to detect a variety of contraband, including shielded nuclear materials, in vehicles and containers at U.S. ports of entry. However, we reported that the office did so without fully understanding that the technology would not fit within existing primary inspection lanes at CBP ports of entry.[i] We identified lessons learned for DHS to consider in its future acquisition efforts, such as to (1) engage in a robust departmental oversight review process, (2) separate the research and development functions from acquisition functions, (3) determine the technology readiness levels before moving forward to acquisition, and (4) rigorously test devices using actual agency operational tactics before making decisions on acquisition. DHS announced the termination of the program in September 2010. DNDO also tested next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials. We reported in June 2009 that while DNDO increased the rigor of testing the new monitors in comparison with previous tests and thereby added credibility to the test results, the benefits of the monitors may not justify the high cost. In July 2011, the Director of DNDO testified that because the original design specification for advanced spectroscopic monitors program does not adequately reflect the operational needs in the field, and because there are now competing commercially-available portal radiation detection systems, DHS was ending the program as originally conceived. DHS reported that it plans to deploy the existing units to field locations to gather operational data to support future planning efforts.

Area	Overall assessment	Summary of key progress and work remaining
		DHS developed and implemented programs to partner with foreign governments to inspect suspicious cargo before it leaves for U.S. ports, but these programs should be improved through enhanced planning such as feasibility analyses and oversight. **Key progress:** DHS implemented programs to inspect suspicious cargo before it leaves for U.S. seaports. For example, CBP established partnerships with members of the international trade community, including the private sector through its Customs-Trade Partnership Against Terrorism, and with foreign governments through its Container Security Initiative and Secure Freight Initiative. The Container Security Initiative program places CBP staff at participating foreign ports to partner with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States, and the Secure Freight Initiative is a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas. DHS reported that, as of July 2011, the Container Security Initiative was operational at 58 ports worldwide. CBP and its international partners also developed the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework). In February 2010, the DHS IG reported on CBP's management and oversight of the Container Security Initiative program. The DHS IG noted that CBP had used proactive management and oversight processes through the Container Security Initiative to identify and inspect high-risk cargo at foreign ports. The IG further reported that CBP conducts periodic evaluations of overseas Container Security Initiative operations and has software tools to help managers monitor port activities. **What remains to be done:** We reported in October 2009 that CBP had made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative program, leaving the feasibility of 100 percent scanning largely unproven. CBP had not developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.[j] Among other things, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning of all U.S.-bound cargo containers in light of the challenges faced at the initial Secure Freight Initiative ports. DHS concurred with our recommendations. Although DHS has not conducted a feasibility analysis, DHS reported that it is examining alternatives to 100 percent scanning as part of the current effort to develop the National Strategy for Global Supply Chain Security, which is intended to articulate an integrated U.S. government vision for collaborating broadly to manage the risks presented by and to the global supply chain. According to DHS, this strategy is undergoing interagency review, and should be issued in the fall of 2011. This strategy should help DHS more fully evaluate various alternatives for implementing the 100 percent scanning requirement or other alternatives that enhance cargo container security in a cost-efficient manner. However, since the strategy is not yet complete, it is too early to assess its impact.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Maritime Security and Response Operations requirements were referred to Operation Neptune Shield requirements until November 2010. They require Coast Guard units to escort a certain percentage of high capacity passenger vessels at each maritime security threat level to protect against an external threat, such as a waterborne improvised explosive device. This requirement is applicable to all types of high capacity passenger vessels—cruise ships, ferries, and excursion vessels—in a sector's area of responsibility.

[b] We are conducting our work for the Senate Committees on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and the House Homeland Security Committee, Subcommittee on Border and Maritime Security.

[c] The Maritime Transportation Security Act of 2002, as amended, establishes requirements for various layers of maritime security, including requiring a national maritime transportation security plan, area maritime transportation security plans, and facility and vessel security plans. The act calls for various types of facilities to develop and implement security plans, and it places federal responsibility for approving and overseeing these plans with DHS. See Pub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2068 (2002) (codified as amended at 46 U.S.C. § 70103). DHS has placed lead responsibility for this and other Maritime Transportation Security Act requirements with the U.S. Coast Guard. Subsequent Coast Guard guidance called for conducting annual on-site inspections and annual unannounced spot checks to verify a facility's compliance with its security plan.

[d] We are conducting our work for the House Committee on Homeland Security and its Subcommittee on Oversight, Investigations and Management; the House Committee on Energy and Commerce; the House Committee on Transportation and Infrastructure; the Senate Committee on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and Representative Edward Markey.

[e] See Pub. L. No. 109-347, § 108(a), 120 Stat. 1884, 1892 (2006) (codified as amended at 46 U.S.C. § 70107A).

[f] We are conducting this work for the Senate Committee on Commerce, Science, and Transportation; the House Committee on Transportation and Infrastructure; and the Senate Committee on Homeland Security and Governmental Affairs.

[g] The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the *International Convention for the Safety of Life at Sea, 1974.* In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

[h] The National Ocean Policy is policy adopted by executive order that includes a set of overarching guiding principles for management decisions and actions toward U.S. oceans, coasts and the Great Lakes. Exec. Order No. 13,547, 75 Fed. Reg. 43,023 (July 19, 2010).

[i] DNDO announced the termination of the Cargo Advanced Automated Radiography System program in September 2010.

[j] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

GAO Contact

For additional information about this area, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

Appendix IX: Immigration Enforcement

What This Area Includes

Source: ICE.

ICE Agents.

The Department of Homeland Security (DHS) is responsible for enforcing U.S. immigration and customs laws, and within DHS, U.S. Immigration and Customs Enforcement (ICE) is primarily responsible for immigration and customs enforcement efforts. ICE's key responsibilities and efforts within immigration enforcement include (1) investigating and taking action to address individuals who have committed immigration and customs offenses, such as overstays;[1] addressing immigration law violations at the workplace; investigating human trafficking and smuggling operations; and combating illicit smuggling of firearms, narcotics, and illicit proceeds; and (2) identifying, detaining, and removing aliens subject to removal.[2] As the primary component responsible for immigration and customs enforcement, for fiscal year 2011 ICE had about 20,000 personnel, and its budget authority was about $5.8 billion.[3] Immigration enforcement falls primarily within the Quadrennial Homeland Security Review Mission 3: Enforcing and Administering Our Immigration Laws.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to immigration enforcement also include the management and training of immigration enforcement human capital, we are not reporting on DHS's progress in this area. Additionally, ICE's customs enforcement efforts include investigations of such offenses as money laundering and other financial crimes. Specifically, ICE reports efforts to address money laundering, including coordinating with federal, state, local, and foreign law enforcement to conduct multi-jurisdictional

[1] Overstays are unauthorized immigrants in the United States who entered the country legally on a temporary basis but then overstayed their authorized periods of admission.

[2] While ICE's immigration enforcement efforts reported by us and the DHS IG primarily fall within Mission 3 of the Quadrennial Homeland Security Review, according to ICE, its efforts to investigate alien smuggling and firearms trafficking fall within Mission 2: Securing and Managing Our Borders as this mission includes disrupting and dismantling transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across United States borders, and commit violent acts. For the purposes of this report, we discussed ICE's alien smuggling and firearms trafficking enforcement efforts under the immigration enforcement functional area aligned under QHSR Mission 3, as discussed in appendix I on our scope and methodology.

[3] Although this appendix focuses primarily on enforcement of immigration laws, the resource amounts provided here encompass all ICE mission areas, including enforcement of customs laws.

criminal investigations targeting organizations involved in the movement and smuggling of illicit proceeds. ICE also reported developing, in collaboration with Mexico, a study of the processes and methods used by transnational criminal organizations to move illicit money from the United States into other countries. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly ICE, expanded its immigration and customs enforcement programs and activities in key areas on which we have reported, such as overstay enforcement, compliance with workplace immigration laws, alien smuggling, and firearms trafficking. For example, ICE increased its resources for investigating overstays 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. Specifically, in April 2011 we reported that DHS increased the E-Verify program's accuracy by expanding the number of databases it can query, took actions to safeguard the privacy of personal information for employees who are processed through E-Verify, and implemented steps to prepare for possible mandatory implementation of E-Verify for all employers nationwide. ICE also expanded its programs for identifying and removing aliens from the United States to include, for example, entering into agreements with state and local jurisdictions to assist in identifying aliens subject to removal. However, our work has shown that work remains in these areas. For example, ICE 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. Moreover, ICE should better leverage opportunities to strengthen its alien smuggling enforcement efforts by assessing the possible use of various investigative techniques, and CBP should better assess progress made in achieving its alien smuggling-related program objectives. We have also reported on weaknesses with the E-Verify program, including challenges in accurately estimating E-Verify costs that put DHS at an increased risk of not making informed investment decisions and developing justifiable budget requests for future E-Verify use and potential mandatory implementation of it. Table 13 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 13: Assessment of Progress and Work Remaining in Key Immigration Enforcement Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Investigations of immigration and customs offenses	DHS dedicated additional resources to overstay enforcement and alien smuggling investigations, and took action to strengthen its voluntary program for helping employers' compliance with immigration laws at the workplace and to combat firearms trafficking. However, DHS lacks measures for assessing the effectiveness of its efforts and should strengthen its investigations by assessing the use of additional investigative techniques, and better ensure that it makes informed investment decisions by developing more reliable cost estimates.	**ICE investigates few overstays, and its efforts should be strengthened by improved planning and performance management.** **Key progress:** ICE took action to address a small portion of the estimated overstay population due to, among other things, competing priorities. In April 2011 we reported that ICE's Counterterrorism and Criminal Exploitation Unit (CTCEU)—the primary federal entity responsible for taking enforcement action to address overstays—prioritizes and assigns overstay cases to field offices for investigation. CTCEU prioritizes in-country overstay leads based on various factors that consider the potential risks overstays may pose to national security and public safety, and field offices investigate those leads that CTCEU identifies as a priority. We reported that field offices had closed about 34,700 overstay investigations that CTCEU headquarters 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.[a] Additionally, we reported that since fiscal year 2006, ICE allocated about 3 percent of its investigative work hours to overstay investigations, but was considering assigning some responsibility for noncriminal overstay enforcement to its Enforcement and Removal Operations directorate to expand its overstay enforcement efforts. **What remains to be done:** In April 2011 we reported that ICE lacked measures for assessing its performance in investigating overstays and the quality of its overstay leads sent to field offices for investigation, making it difficult for ICE management to assess program performance and make decisions for program improvements. Among other things, we recommended that ICE establish a time frame for completing overstay enforcement planning and develop measures for assessing the performance and progress of its overstay enforcement efforts. ICE concurred with these recommendations and reported that it planned to take action to address them, such as working with national security partners to determine possible performance measures. In August 2011, ICE reported that it had efforts underway to develop qualitative and quantitative measures related to lead quality, cost effectiveness, process efficiency, and risk, and plans to implement the measures in fiscal year 2012. ICE further reported that it had initiated new targeting methods intended to better ensure it targets leads that pose the greatest security and public safety risks. While these are positive steps, ICE is in the early stages of implementing them and thus, it is too early to assess their effectiveness.
		DHS took steps to improve compliance with immigration laws at the workplace, but a key tool for verifying work eligibility is vulnerable to inconsistent recording of information and unreliable cost estimates. **Key progress:** DHS has taken 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. Specifically, in April 2011 we reported that DHS increased the E-Verify program's accuracy by expanding the number of databases it can query, took actions to safeguard the privacy of personal information for employees who are processed through E-Verify, and implemented steps to prepare for possible mandatory implementation of E-Verify for all employers nationwide. Moreover, in July 2011, DHS reported additional improvements to E-Verify, including initiatives to reduce identity fraud, such as launching a pilot program in one state that will allow E-Verify to confirm the validity and authenticity of driver's licenses used by employees.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported that the E-Verify program continues to face challenges. For example, we reported that the accuracy of E-Verify is limited by inconsistent recording of employees' names and fraud, and that, because of challenges in accurately estimating E-Verify costs, DHS is at an increased risk of not making informed investment decisions, understanding system affordability, and developing justifiable budget requests for future E-Verify use and potential mandatory implementation of it. Among other things, we recommended that DHS disseminate information to employees on the importance of consistently recording their names, and that DHS ensure that a life cycle cost estimate for E-verify is developed in a manner that reflects the characteristics of a reliable estimate—comprehensive, well-documented, accurate and credible. DHS concurred with these recommendations and reported taking steps toward addressing them, such as disseminating information through various media—guides, websites, videos, and a toll-free employee hotline—to emphasize the importance of recording employees' names consistently and to respond to employee issues. In July 2011, DHS also reported that it was in the final stages of finalizing a life-cycle cost estimate for the program. As DHS is in the early stages of implementing these efforts and has not yet completed its cost estimate, it is too early to assess their impact.
		DHS expanded alien smuggling resources, but should better leverage program resources. **Key progress:** DHS increased its resources for investigating and interdicting alien smuggling activities. In May 2010 we reported that U.S. Customs and Border Protection (CBP) is responsible for interdicting smuggled aliens as illegal border-crossing attempts are made between the ports of entry.[b] CBP maintains several programs that address alien smuggling and collaborates with ICE in providing information for alien smuggling investigations obtained during interdictions. We also reported that ICE work years spent investigating alien smuggling increased from 190 to 197 from fiscal years 2005 through 2009. Furthermore, in May 2010 we reported that ICE and CBP had established objectives for their alien smuggling related enforcement programs, such as objectives to remove aliens who are apprehended during the dangerous summer months to deter them from returning in order to reduce loss of life and disrupt alien smuggling operations.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported that ICE and CBP had opportunities to improve efforts to address alien smuggling. Specifically, we reported that ICE should better leverage resources for its alien smuggling investigative efforts by, among other things, assessing the (1) possible expansion of a program for handling state and local law enforcement referrals, including smuggling cases, to help ICE direct more resources toward alien smuggling investigations; and (2) possible use of investigative techniques to follow cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. We also reported that CBP should improve its efforts by better evaluating its progress in meeting its alien smuggling objectives. We recommended, among other things, that DHS evaluate the feasibility of expanding the ICE response program, assess investigative strategies, and establish a plan, including performance measures, for evaluating alien smuggling related enforcement programs. DHS generally concurred with these recommendations and reported actions planned or underway to implement them. For example, in July 2011 CBP reported developing draft performance measures for its alien smuggling-related enforcement programs that are awaiting approval from CBP management. In addition, ICE reported studying the feasibility of expanding the response program and possible use of financial investigative techniques; however, ICE stated that expansion of the program is contingent upon fiscal year 2012 budget decisions. These are positive steps that should strengthen ICE and CBP efforts to address alien smuggling. However, since these efforts are not yet complete, we have not assessed their impact.
		ICE took action to implement its firearms trafficking responsibilities. **Key progress:** In June 2009, we reported that ICE developed its Border Enforcement Security Task Force initiative to help facilitate cooperation and bring together resources of ICE, CBP, and other United States and Mexican law enforcement entities to focus investigative, interdiction, and intelligence assets towards the identification, prioritization, and investigation of emerging or existing threats to our border, such as the investigation of illicit smuggling of people and goods, including firearms. In July 2011, ICE reported various initiatives to further increase interaction and collaboration with its law enforcement partners, such as assigning an analyst to the El Paso intelligence center, which serves as a central repository for weapons-related intelligence information; increasing the number of personnel assigned to Border Enforcement Security Task Forces; and establishing a virtual task force through which United States and Mexican law enforcement can share information regarding weapon seizures.

Area	Overall assessment	Summary of key progress and work remaining
		We also reported on challenges with ICE's firearms trafficking efforts, which ICE addressed. For example, we reported that ICE could help enhance interagency collaboration in combating arms trafficking to Mexico.[c] Specifically, we found that ICE and the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—the primary agencies implementing efforts to address illicit sales of firearms—did not effectively coordinate their efforts, in part, because the agencies lacked clear roles and responsibilities and had been operating under an outdated interagency agreement, resulting in instances of duplicate initiatives and confusion during operations. Additionally, ICE, along with other agencies, had not systematically gathered, analyzed, and reported data that could be useful to better understand the nature of the firearms trafficking problem, help plan ways to address it, and assess progress made, hampering the investigative capacity of the law enforcement agencies involved. Among other things, we recommended that DHS work with the Department of Justice to finalize the memorandum of understanding they were working on between ICE and ATF. We also recommended that ICE and ATF develop processes for periodically monitoring implementation of the memorandum's provisions so as to make any necessary adjustments and ensure the systematic gathering and reporting of data related to results of enforcement efforts, including firearms seizures, investigations, and prosecutions. DHS agreed with our recommendations and has taken actions and has others underway that should address them. For example, in June 2009 ICE and ATF signed a memorandum of understanding to, in part, formalize their partnership and coordinate collective law enforcement efforts. In addition, ICE developed a system to help ensure oversight and determine whether changes are needed to implement the memorandum. ICE also reported planning to enhance its databases to better capture and track data on enforcement efforts.
Identification, detention, and removal of aliens subject to removal	ICE expanded its programs to identify and remove incarcerated aliens who are eligible for removal.	**ICE 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.** **Key progress:** In January 2009 we reported that through ICE's 287(g) program—in which ICE enters 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—ICE reported enrolling 67 state and local law enforcement agencies and training 951 state and local law enforcement officers.[d] According to data provided by ICE for 25 of the 29 program participants we reviewed, during fiscal year 2008, about 43,000 aliens had been arrested pursuant to the program.[e] We also reported that ICE had designed some management controls for the 287(g) program, such as memorandums of agreement to govern program implementation and background checks for state and local law enforcement officers. Furthermore, in April 2011, ICE established its 287(g) Communications Plan to provide clear and consistent information about the 287(g) program including the program's goals and policies, among other things. In March and September 2010, the DHS IG reported, in part, that ICE and state and local law enforcement agencies had not complied with all terms of the 287(g) agreements, and the program's performance measures did not always align with program priorities.[f] Similarly, in January 2009 we reported that although ICE had established some management controls for the 287(g) program, it lacked other controls such as documented program objectives to help ensure that participants work toward a consistent purpose. We also reported that ICE lacked performance measures to fully evaluate the 287(g) program, making it difficult for ICE to ensure that the program was operating as intended.

Area	Overall assessment	Summary of key progress and work remaining
		We and the DHS IG made a number of recommendations to ICE to help address these challenges, which DHS has worked to address. For example, DHS specified in its memorandum of agreement with state and local law enforcement the data that each agency is expected to collect regarding their implementation of the 287(g) program so that ICE can better ensure it has information with which to gauge program results. ICE also put into place controls for the program. Moreover, in May 2011 DHS established performance measures in its 287(g) Strategic Plan for fiscal years 2011-2016, and detailed the process for 287(g) jurisdictions to collect performance data in its Program Performance Measures Guide.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] 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).

[b] Ports of entry are government-designated locations where CBP inspects persons and goods to determine whether they may be lawfully admitted into the country. A land port of entry may have more than one border crossing point where CBP inspects travelers for admissibility into the United States.

[c] Agencies with programs related to arms trafficking include, but are not limited to, DHS's ICE and CBP; the Department of Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives, Drug Enforcement Administration, and the Executive Office for U.S. Attorneys; the Department of State; and the Office of National Drug Control Policy.

[d] The program is named after section 287(g) of the Immigration and Nationality Act, which authorizes the agreements with state and local law enforcement agencies and is codified at 8 U.S.C. §1357(g).

[e] In August 2011, ICE reported a revised estimate of about 46,000 aliens being arrested pursuant to the program in fiscal year 2008.

[f] According to the 287(g) agreement, state and local law enforcement agencies are to identify and initiate removal of criminal aliens based on ICE's top priorities. Specifically, the 287(g) agreement identifies three categories of aliens that are a priority for arrest and detention. The highest priority, Level 1, consists of aliens who have been convicted of or arrested for major drug or violent offenses. Level 2 includes aliens who have been convicted of or arrested for minor drug or property offenses. Level 3 includes aliens who have been convicted of or arrested for other offenses.

GAO Contact

For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

Appendix X: Immigration Services

What This Area Includes

Source: Department of Defense.

Service Members Who Became U.S. Citizens During a Naturalization Ceremony Held at the Al Faw Palace in Baghdad, Iraq.

Within the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is the agency primarily responsible for providing immigration services in the United States and internationally at U.S. embassies, consulates and refugee centers. USCIS's key responsibilities and efforts within immigration services include:

- administering immigration benefits, such as processing millions of applications and petitions received each year for about 50 types of immigration benefits for persons seeking to study, work, visit, or live in the United States, and to become U.S. citizens; and
- detecting and resolving suspicious information about and reviewing evidence provided by benefits applicants and petitioners and referring them for fraud investigation and possible sanctioning by other DHS components or external agencies, as appropriate.

As the primary component responsible for immigration services, for fiscal year 2011 USCIS had about 12,000 personnel, and its budget authority was about $2.6 billion. Immigration enforcement falls primarily within the Quadrennial Homeland Security Review Mission 3: Enforcing and Administering Our Immigration Laws.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to immigration services also include immigrant integration, we have not reported on DHS's progress and work remaining in this area. According to USCIS documentation provided to us in July 2011, the agency has undertaken initiatives to support immigrant integration, particularly related to citizenship, including, among other things, outreach, grants for education programs, and improved tools and resources on the citizenship and naturalization process. We currently have work underway for the House Committee on Homeland Security assessing USCIS's immigrant integration efforts, and plan to report on the results of our work later this year.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly USCIS, improved the quality and efficiency of the immigration benefit administration process, and strengthened its immigration fraud detection and deterrence efforts. For example, USCIS 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. In September 2008 we reported that the USCIS Asylum Division designed training programs and quality reviews to help ensure the integrity of asylum adjudications. In addition, 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.[1] Further, in July 2011, USCIS reported that it completed the development of a database for analyzing fraud—the Fraud Detection and National Security Data System—which it uses to collect data on fraud and national security concerns. In addition, among other things, USCIS implemented the Administrative Site Visit and Verification Program, through which it conducts pre-and post-adjudication site visit inspections to verify information contained in certain visa petitions.

However, our work and that of the DHS IG have shown that work remains in these areas. For example, USCIS'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 preparing key DHS acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process. USCIS should also take additional action to address vulnerabilities identified in its assessments intended to determine the extent and nature of fraud in certain applications. Further, in September 2008 we reported that, despite mechanisms USCIS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers cited challenges in identifying fraud as a key factor affecting their adjudications. Table 14 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[1]The Fraud Detection and National Security Directorate was originally established as an office within the USCIS. In January 2010, the USCIS director elevated the office to directorate level in order to bring greater focus to USCIS's anti-fraud and national security responsibilities.

Table 14: Assessment of Progress and Work Remaining in Key Immigration Services Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Administration of immigration benefits	USCIS initiated efforts to improve the quality and efficiency of its administration of immigration benefits by, among other things, working to transition to an electronic process. However, these efforts have been hampered by management challenges, such as insufficient planning. In addition, preliminary observations from our ongoing work assessing USCIS transformation efforts indicate that USCIS has missed its planned milestones by more than 2 years, and has not adhered to DHS acquisition rules, including not preparing key acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process.	**USCIS has efforts underway to modernize its benefit administration processes, but these efforts have been hampered by challenges in planning, and preliminary observations from our ongoing work indicate that USCIS has not adhered to DHS acquisition rules.** **Key progress:** Through its transformation initiatives, USCIS aims to upgrade its current, paper-based data systems, which are fragmented, expensive to handle, and prone to handling errors, into a digital processing resource to enhance customer service, improve efficiency with expanded electronic filing, and prevent future backlogs of immigration benefit applications. In July 2007, we reported that USCIS was in the early stages of its Transformation Program and that it had drafted a strategic plan to guide its modernization efforts and established a Transformation Program Office to oversee and carry out the effort. We reported that USCIS's plans partially or fully addressed most key practices for organizational transformations (e.g., by establishing a mission, vision, and integrated strategic goals). **What remains to be done:** In July 2007, we identified challenges in USCIS's transformation plans that created risks that could undermine its success. For example, we reported that the lack of clear and measurable performance measures and targets for the transformed agency put it at risk of developing or selecting new business processes and systems and services that would not achieve the goals of the transformation. Subsequently, in July 2009, the DHS IG found that USCIS positioned itself to better plan and prepare for the next phase in the agency's transformation, including establishing a strategy for deploying the transformed business capabilities and implementing the transformation program. USCIS also implemented pilot programs to test the viability of a number of system capabilities required for the transformation. However, the DHS IG also reported that the success of these pilots had been restricted by factors such as ineffective planning and limited evaluation. Among other things, we recommended that USCIS document specific outcome-oriented performance measures that are aligned with its goals, and the DHS IG recommended that USCIS complete evaluations to document the results and lessons learned from the pilots.[a] USCIS generally concurred with these recommendations and took action to address some and is in the process of addressing others. For example, in July 2010, USCIS reported that it had approved four performance measures that align with its transformation goals, and in July 2011 it reported that it was in the process of developing associated targets for these measures as well as interim measures to gauge usage, customer service, accuracy, and timeliness throughout deployment of the transformed system. In addition, USCIS documented lessons learned from the pilots and stated that it planned to document lessons learned from all future pilots.

Area	Overall assessment	Summary of key progress and work remaining
		We currently have work underway evaluating USCIS's efforts to implement the Transformation Program.[b] Our preliminary observations indicate that UCSIS has not consistently adhered to DHS acquisition guidance. For example, USCIS did not prepare key acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process. USCIS does not agree that the agency did not consistently adhere to DHS acquisition guidance because the agency asserts that it produced all documents called for by the guidance. While we agree that USCIS eventually produced the documents, it did not do so before contracting to obtain the needed capabilities as directed by the guidance, and therefore, did not adhere to the guidance. In addition, scheduled deployment of the program's new electronic immigration system is over 2 years behind schedule and by the end of September 2011, USCIS estimates it will have spent about $770 million since the program began in 2006. According to USCIS, the program's delays can be attributed to changes in departmental acquisition policies and a December 2009 decision to modify the planned sequence of deliverables, among other things. USCIS also reported that DHS slowed the program's overall schedule to enhance oversight and better mitigate program risks. Moving forward, improved acquisition planning, including having reliable program schedules, could help USCIS avoid further delays and potential cost overruns. We plan to report on the final results of this review later this year.
		DHS took steps to ensure quality in its application adjudication processes, but encountered challenges, particularly with regard to training. **Key progress:** In February 2008, we reported that the USCIS Humanitarian Affairs Branch designed internal controls to help ensure that requests for humanitarian parole were decided in accordance with applicable guidelines, such as clear and detailed written policies and procedures.[c] However, we also reported that the USCIS Humanitarian Affairs Branch did not have a training program for new staff and staff who may be detailed to process applications, which was essential to ensure that criteria for granting and denying parole were applied consistently and fairly by the adjudicators.[d] We recommended that USCIS develop a training program curriculum on adjudication of humanitarian parole cases for new and detailed staff. In response to our recommendation, USCIS developed a training program and standardized training materials for adjudicating humanitarian parole cases, which it reported implementing in February 2009. Further, in September 2008 we reported that the USCIS Asylum Division had designed training programs and quality reviews to help ensure the integrity of asylum adjudications, such as centralized training for officers that addressed most facets of the asylum adjudication process. In addition to these efforts, in July 2011, USCIS provided us with information on other programs and efforts it has underway to help strengthen its administration of immigration benefits. For example, to help prevent future immigration benefit application backlogs from accruing, USCIS reported that it had developed a tool to identify USCIS offices with additional capacity to adjudicate benefits applications. USCIS indicated that it could shift work from offices with backlogs to offices with additional capacity when needed. USCIS also has developed a forecasting model that projects application receipts to help USCIS anticipate and plan for seasonal application surges. We have not completed work in these areas upon which to make an assessment of USCIS's progress.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In September 2008 we reported that the USCIS Asylum Division lacked key information for making training decisions because it did not consistently solicit input from asylum officers and supervisors on a range of their training needs.[e] We recommended that DHS develop a framework for soliciting information on asylum adjudicators' training needs. DHS concurred with our recommendation and has actions underway to address it. For example, USCIS developed an online training needs assessment that was completed by asylum officers and supervisors between July and August 2010. In July 2011, USCIS reported that it had used the results of the assessment to identify training needs at the national and local levels, and based on these needs, has begun to deploy local training initiatives. While these are positive steps, DHS is in the process of deploying these local training initiatives, and thus, it is too early to assess their results. As we previously reported, supplementing existing training should improve asylum officers' ability to elicit needed information during an applicant interview to help distinguish between a genuine and fraudulent claim.
Immigration benefit fraud	DHS implemented programs and activities for detecting and deterring immigration fraud, but work remains to improve their impact, such as assisting adjudication officers with improving their ability to identify fraud and addressing vulnerabilities identified through USCIS fraud assessments.	**DHS implemented programs and activities for detecting and deterring immigration fraud, but work remains to improve their impact, such as assisting adjudication officers with improving their ability to identify fraud and addressing vulnerabilities identified through USCIS fraud assessments.** **Key progress:** DHS implemented programs for resolving issues related to immigration petitions and applications with potential immigration benefit fraud indicators.[f] In April 2008, the DHS IG reported that the USCIS Fraud Detection and National Security Directorate had identified general strategies for (1) obtaining from adjudicators all petitions with fraud indicators, or articulable fraud, and referring them to U.S. Immigration and Customs Enforcement (ICE) for review; (2) developing a database to enhance the office's ability to analyze fraud; (3) tracking all petitions with articulable fraud indicators from referral to completion; and (4) identifying and analyzing fraud patterns and trends using data mining and pattern recognition to search new immigration petitions against known fraud indicators.[g] In July 2011, USCIS reported that it had completed the development of a database for analyzing fraud—the Fraud Detection and National Security Data System—and uses this system to collect data on fraud and national security concerns. In addition, USCIS reported taking additional steps to enhance its fraud detection and deterrence efforts. These included placing Fraud Detection and National Security Immigration Officers in domestic USCIS offices and in three overseas locations to provide onsite investigations capabilities; developing an intelligence component to share information within and outside of DHS to help develop investigations about individuals who pose a public safety or national security risk; and creating a Threat Assessment Branch to, among other things, provide oversight of fraud detection operations at USCIS centers. USCIS further reported implementing the Administrative Site Visit and Verification Program, through which it conducts pre-and post-adjudication site visit inspections to verify information contained in certain visa petitions, and implementing the Validation Instrument for Business Enterprises Program, through which it uses a Web-based instrument to validate basic information about companies or organizations petitioning to employ alien workers. We have not completed work in these areas upon which to make an assessment of USCIS's progress.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In December 2008 we reported that USCIS needed to take actions to address vulnerabilities in its process for granting permanent residency. For example, USCIS worked to address vulnerabilities identified in two of its assessments intended to determine the extent and nature of fraud in certain application types that may lead to permanent residency, such as increasing site visits and requirements to verify the legitimacy of institutions petitioning for benefits for religious workers. However, USCIS had not released reports on three other benefit fraud and compliance assessments and had not completed actions to address vulnerabilities identified in four assessments. These assessments indicated, for example, that some asylum applicants submitted false arrest and medical reports to support their claims of persecution, and some such fraudulent applications had been approved by USCIS adjudicators. We concluded that the vulnerabilities identified by these assessments, such as failure to verify the evidence applicants and their petitioners provide, would persist until USCIS took corrective actions, thereby increasing the risk that ineligible individuals would obtain lawful permanent resident status. Further, in September 2008 we reported that, despite mechanisms USCIS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers 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. We also found that assistance from other federal entities to asylum officers in assessing the authenticity of asylum claims had been hindered in part by resource limitations and competing priorities. We recommended that, among other things, USCIS prepare a roadmap for each of the four outstanding benefit fraud and compliance assessments that delineates timetables for deciding what actions to take, which USCIS organizational units will be responsible for implementing, and a timetable for implementing agreed-upon actions. We also recommended that, in order to help asylum officers refine their interview techniques to elicit information to use in assessing credibility, determining eligibility, and distinguishing between genuine and fraudulent claims, the Asylum Division explore ways to provide additional opportunities for asylum officers to observe skilled interviewers. DHS agreed with these recommendations, has addressed some, and has actions underway to address others. For example, USCIS developed a draft plan for asylum officer interview observation opportunities to occur quarterly, and reported in July 2011 that it was continuing to explore different models for interview observations. In addition, in July 2011, USCIS reported that it had established a Fraud Detection and National Security component within the Refugee, Asylum, and International Operations Directorate in order to improve fraud detection and prevention capabilities across the directorate, which includes the Asylum Division. With respect to addressing vulnerabilities identified in its outstanding benefit fraud and compliance assessments, in August 2011, USCIS officials told us that USCIS was in the process of hiring a contractor to assist with the effort of revising how these assessments were conducted, and that the review and timetable for implementing actions related to the outstanding assessments would depend on the contractor's findings. USCIS further reported that the procurement for the contractor was underway. Once the assessments are reviewed, USCIS expects to begin implementing our recommendation to develop roadmaps for addressing their findings.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Outcome-oriented performance measures show results or outcomes related to an initiative or program in terms of its effectiveness, efficiency, or impact.

[b] We are conducting this work for the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on the Judiciary, and the Senate Committee on the Judiciary.

[c] The Humanitarian Affairs Branch was formerly called the Humanitarian Assistance Branch.

[d] Aliens who are otherwise inadmissible but have an urgent humanitarian need may apply to USCIS's Humanitarian Affairs Branch for humanitarian parole, which permits an alien to enter the United States on a temporary basis.

[e] Each year tens of thousands of noncitizens apply in the United States for asylum, which provides refuge to those who have been persecuted or fear persecution. The Asylum Division within USCIS is responsible for adjudicating these applications.

[f] Benefit fraud might involve a conspiracy in which an organization profits from thousands of fraudulent applications, or what DHS refers to as "single-scope fraud," such as two individuals agreeing privately to a fraudulent marriage.

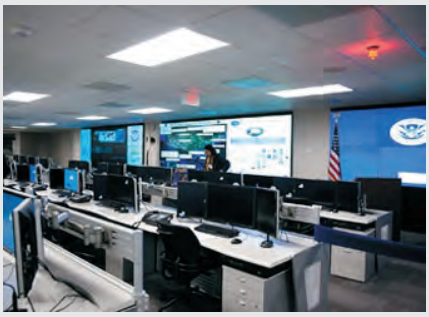
[g] Articulable fraud encompasses any application with concrete evidence that leads the adjudicator to suspect fraud, such as contradictory statements on material facts, atypical or boilerplate applications, or suspected fraudulent documents. Pursuant to a September 2008 memorandum of agreement between USCIS and ICE, USCIS no longer refers all fraud cases to ICE. Rather, USCIS refers those cases that are most likely to result in criminal investigations to ICE and investigates the remaining cases itself.

GAO Contact

For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

Appendix XI: Critical Infrastructure Protection—Cyber Assets

What This Area Includes



Source: NPPD.

Operations Center.

The Department of Homeland Security (DHS) has overall responsibility for coordinating critical infrastructure protection efforts for 18 critical infrastructure sectors—such as energy, water, and communications. Within DHS, the National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) is charged with enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C's key responsibilities and efforts related to cybersecurity include (1) risk assessment and planning; (2) protection and resiliency; and (3) partnerships and coordination mechanisms. As the primary DHS component responsible for safeguarding physical and cyber assets, in fiscal year 2011 NPPD, which includes CS&C, had about 2,800 personnel and its budget authority was about $2.3 billion.[1] Critical infrastructure protection of cyber assets primarily falls within the Quadrennial Homeland Security Review Mission 4: Safeguarding and Securing Cyberspace.

In 1997 we designated federal information security as a high-risk area, and in 2003 we expanded this area to include cyber critical infrastructure protection. In designating these issues as high-risk, we reported that federal agencies and our nation's critical infrastructure—such as power distribution, water supply, telecommunications, and emergency services—rely extensively on computerized information systems and electronic data to carry out their operations. The security of these systems and data is essential to protecting national and economic security, and public health and safety. Safeguarding federal computer systems and the systems that support critical infrastructure—referred to as cyber critical infrastructure protection—is a continuing concern. In our January 2009 high-risk update, we reported that federal agencies made progress in strengthening information security, but that most agencies continued to experience significant deficiencies that jeopardize the confidentiality, integrity, and availability of their systems and information. We also reported that DHS, as the focal point for federal efforts to protect the nation's critical infrastructure continued to make progress in fulfilling its key cyber critical infrastructure protection responsibilities. However,

[1] The goal of the NPPD is to advance the Department's risk-reduction mission. CS&C is within NPPD. Other divisions or offices within NPPD include, for example, the Federal Protective Service and the Office of Infrastructure Protection. The NPPD budget authority for fiscal year 2011 includes $1.3 billion in appropriated funds, and the authority to collect another $1.1 billion in fees for the Federal Protective Service. These values do not add up to $2.3 billion due to rounding.

but in the February 2011 high-risk update we identified several areas of responsibility that required further attention, such as advancing cyber analysis and warning capabilities, acquiring sufficient analytical and technical capabilities, and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure. In January 2011, DHS provided us with a corrective action plan for this high-risk area. We provided DHS with feedback on this plan noting, for example, that the plan included objectives, milestones, and planned accomplishments related to DHS's cybersecurity responsibilities. However, we identified aspects of the plan that should be strengthened, such as clarifying whether DHS's 2010 goals and objectives for its corrective actions were met, and identifying resources needed and planned milestones for 2011 activities.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has other ongoing efforts related to cyber critical infrastructure protection, such as the assessment of cybersecurity measures implemented at high-risk chemical facilities as part of its Chemical Facility Anti-Terrorism Standards program, on which we have not reported. DHS also established the National Cybersecurity and Communications Integration Center in October 2009 to serve as a national cyber and communications operations center to fuse information from federal civilian agencies, law enforcement, intelligence, state and local government, and the private sector. Further, DHS signed a memorandum of agreement with the Department of Defense to improve cyber coordination.[2] In addition, according to DHS officials, NPPD's Office of Infrastructure Protection and the National Cyber Security Division collaborated to integrate cybersecurity elements into the Office of Infrastructure Protection's facility security and vulnerability assessments. The National Cyber Security Division also conducts cyber assessments in support of the Office of Infrastructure Protection's Regional Resiliency Assessment Program and major national events, according to DHS. We have not completed work on these areas upon which to make an assessment of DHS's progress.

[2] The Department of Defense also has responsibilities for cybersecurity efforts.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS expanded its efforts to conduct cybersecurity risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cybersecurity partnerships and coordination mechanisms. For example, DHS updated the *National Infrastructure Protection Plan* to include an emphasis on cybersecurity issues by listing progress made and new initiatives related to cybersecurity. In addition, DHS 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. Additionally, the agency 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. DHS is also working to improve cyber-related partnerships with public and private stakeholders by developing new information-sharing arrangements and addressing corrective actions based on a cybersecurity exercise. In September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing lessons it had learned from these efforts to strengthen public and private incident response capabilities.

However, our work and that of the DHS IG has also shown that key challenges remain in these 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. DHS also faces challenges in fully establishing a comprehensive national cyber analysis and warning capability. For example, in July 2008, we reported that the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. Moreover, the DHS IG reported that DHS needs to establish a consolidated, multiple classification level portal that can be accessed by federal partners with real-time incident response related information and reports. 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. We also reported that public sector stakeholders believed that improvements could be made by improving private sector sharing of sensitive information. Table 15 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 15: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Cyber Assets Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS updated the *National Infrastructure Protection Plan* to include an emphasis on cybersecurity issues, including methodologies to identify systems or networks of national significance. In addition, DHS met and worked with lead federal agencies to update sector specific plans with the goal of fully addressing cyber-related requirements. Most agencies updated their respective plans, and it is important that the plans address cybersecurity requirements.	**DHS placed a greater emphasis on cybersecurity issues in the updated *National Infrastructure Protection Plan*, and directed lead federal agencies to address cybersecurity issues in sector specific plans and sector risk assessments. Most agencies updated their respective plans, and it is important for these updated plans to address cybersecurity requirements to provide information on the implementation of cyber-related protective measures.** **Key progress:** DHS included a greater emphasis on cybersecurity in the 2009 *National Infrastructure Protection Plan* than it did in the first iteration of the plan in 2006. The plan provides the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. In March 2010 we reported that the new 2009 plan lists the progress made and new initiatives related to cybersecurity, including the development of cross-sector cyber methodologies to identify systems or networks of national significance; the addition of a cross-sector cybersecurity working group; and a public-private cross-sector program specifically for cybersecurity. The plan also identified new responsibilities for critical infrastructure partners to conduct cybersecurity exercises to test the security of cyber systems, as well as the development of cybersecurity-specific vulnerability assessments by DHS. In addition, 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. Further, following the publication of the 2009 *National Infrastructure Protection Plan*, DHS directed sector specific agencies to give additional attention to cybersecurity when developing their sector specific plans and sector annual reports.[a] These plans provide the means by which the *National Infrastructure Protection Plan* is implemented across the sectors and articulate the progress of the sectors' critical infrastructure protection and resiliency efforts, challenges, and needs respectively. Regarding cybersecurity, the guidance calls for the sector specific agencies to include goals or long-term objectives for cybersecurity in their sector and explain their approach for identifying their sector's cyber assets, systems, networks, and functions; incorporating cyber elements into sector risk assessments; and prioritizing cyber elements—such as communication and computer networks—of the sector, among other things, as appropriate to each sector.[b] **What remains to be done:** In September 2009 we reported that, among other things, sector-specific agencies had not yet updated their respective sector-specific plans to fully address key DHS cybersecurity criteria. In addition, most agencies had not updated the actions and reported progress in implementing them as called for by DHS guidance. We found that of the 17 sector-specific plans, 9 had been updated, of which 3 addressed DHS's cybersecurity criteria. We noted that these shortfalls were evidence that the sector planning process had not been effective and thus left the nation in the position of not knowing its status in securing cyber critical infrastructure.

Area	Overall assessment	Summary of key progress and work remaining
		We recommended that DHS (1) assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure, and consider whether other options would provide more effective results; and (2) collaborate with the sectors to develop plans that fully address cybersecurity requirements. DHS concurred and reported, for example, that it worked with sector officials to update sector plans with the goal of fully addressing cyber-related requirements. In 2010, the sectors issued 18 updated plans to be reviewed by federal agencies, such as the Office of Management and Budget and DHS. As of August 2011, DHS officials stated that 17 plans were finalized and 1 was in the process of being reviewed. DHS officials were not able to provide milestones for when the remaining plan would be finalized, as it is under federal interagency review. We have not yet reviewed these plans to determine the extent to which they address specified security requirements. Having plans with complete updates that address cybersecurity requirements will be important in providing the nation with information on where we are in implementing associated protective measures designed to secure and protect the nation's cyber and other critical infrastructure.[c]
Protection and resiliency	DHS took steps to secure external network connections in use by the federal government, and to coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. However, to expand protection and resiliency efforts, concerted effort is needed to consolidate and secure Internet connections at federal agencies. DHS also faces challenges in establishing a comprehensive national cyber analysis and warning capability.	**DHS enhanced the protection and resiliency of federal computer networks, but a concerted effort is needed to consolidate and secure Internet connections at federal agencies.** **Key progress:** To reduce the threat to federal systems and operations posed by cyber attacks on the United States, the Office of Management and Budget launched, in November 2007, the Trusted Internet Connections initiative. In 2008, DHS's National Cybersecurity Protection System, operationally known as Einstein, became mandatory for federal agencies as part of this initiative.[d] In March 2010, we reported on federal agencies' efforts to meet the requirements of the Trusted Internet Connections Initiative, which is directed by the Office of Management and Budget with assistance from DHS.[e] Although agencies were in the process of implementing the initiative, we reported that it was resulting in benefits to agencies including improved security and network management. In 2008, DHS developed Einstein 2, which incorporated network intrusion detection technology into the capabilities of the initial version of the system.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: Although we found that agencies reported benefits from the Trusted Internet Connection Initiative, none of the 23 agencies we reviewed met all of the requirements of the Trusted Internet Connections Initiative, as of September 2009.[f] Most agencies reported that they have made progress toward reducing their external connections and implementing critical security capabilities, but they also experienced delays in their implementation efforts.[g] Further, agencies had not demonstrated that they fully implemented the required security capabilities. Agencies had been challenged in implementing the initiative, in part because DHS did not always respond to agency queries on security capabilities in a timely manner. Agencies' experiences with implementing the initiative offered DHS lessons learned, such as the need to define program requirements before establishing deadlines, and the usefulness of sponsoring collaborative meetings for agencies' implementation efforts. In addition, because DHS did not conduct direct testing of the critical security capabilities or evaluate all possible locations in its validation reviews, we concluded that it could not be assured that all critical security capabilities had been implemented. Among other things, we recommended that DHS enhance Trusted Internet Connections' compliance validations by including (1) direct testing and evaluation of the critical capabilities, and (2) evaluation of the capabilities at all agency Trusted Internet Connections locations. DHS concurred with our recommendations and stated that it was taking steps to address them, such as developing and deploying two tools in 2011—one that automates cybersecurity compliance validation, and one that identifies which government owned Internet domains are in compliance with federal guidelines. In July 2011 DHS reported that it conducted assessments that included direct testing of critical security capabilities. However, we have not yet assessed these efforts, as DHS recently conducted this direct testing and is in the process of implementing these two tools. In addition, we reported that DHS had started to deploy Einstein to federal agencies, but faced challenges with meeting program goals. The U.S. Computer Emergency Readiness Team created Einstein in 2003 with the intention to provide DHS with an increased awareness of computer network traffic activity, including possible security incidents, on federal networks by providing intrusion detection capabilities that allow DHS to monitor and analyze agencies' incoming and outgoing Internet traffic. Agencies that participated in Einstein 1 improved identification of incidents and mitigation of attacks. However, as of September 2009, fewer than half of the 23 agencies we reviewed had executed the required agreements with DHS. We identified several challenges that DHS faced regarding deploying Einstein 2, including understanding the extent to which its objective is being met because DHS lacks performance measures for Einstein 2 that address whether agencies report if the alerts represent actual incidents. We also determined that Einstein could fail to fully meet the objective of increasing U.S. Computer Emergency Readiness Team's situational awareness because DHS did not always ensure that key agreements were executed with agencies. We recommended, among other things, that DHS develop additional performance measures that indicate how agencies respond to alerts. DHS concurred and in July 2011 stated that it is taking actions to develop performance measures. As DHS is in the process of developing these measures, it is too early to assess their results. Performance measures will be important in helping DHS understand how agencies respond to alerts.

Area	Overall assessment	Summary of key progress and work remaining
		In addition, DHS officials stated that the department piloted Einstein 3 (the Comprehensive National Cybersecurity Initiative 3), which is intended to be an intrusion prevention system that is to automatically detect and respond appropriately to cyber threats before harm is done. According to DHS officials, once fully deployed, Einstein 2 and 3 will provide cyber protection capabilities to more than 110 federal civilian executive branch departments and agencies. As of July 2011, DHS reported that Einstein 2 was deployed at 16 of 19 access provider agencies and active at 15 of them, and that it is fully deployed and active at each of the 4 private telecommunications service providers through which non-access provider agencies seek Managed Trusted Internet Protocol Services.[h] Taking steps to expand cyber protection capabilities to additional federal departments and agencies should help to improve the nation's cyber infrastructure if those capabilities are implemented effectively. However, we have not yet assessed the effectiveness of these efforts as DHS is in the process of deploying Einstein 2 and 3.
		With the establishment of the U.S. Computer Emergency Readiness Team, DHS took steps to coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. However, DHS faces challenges in establishing a comprehensive national cyber analysis and warning capability. **Key progress:** When incidents such as data loss or theft, computer intrusions, and privacy breaches occur, agencies are to notify the U.S. Computer Emergency Readiness Team. Over the past 5 years, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team has increased; from 5,503 incidents in fiscal year 2006 to 41,776 incidents in fiscal year 2010, an increase of over 650 percent. We currently have work underway assessing the adequacy and effectiveness of agency information security policies and practices, and agencies' implementation of the Federal Information Security Management Act of 2002 requirements, and plan to report on our results later this year.[i] **What remains to be done:** In July 2008, we reported that 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. We recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS generally concurred and stated that it is taking steps to implement them, such as opening two 24-hour centers to increase communication channels and organize cyber response efforts.[j] We are currently working with DHS officials to more fully determine the status of their efforts to address these recommendations.

Area	Overall assessment	Summary of key progress and work remaining
		The DHS IG also identified challenges with the U.S. Computer Emergency Readiness Team analysis and warning program, which DHS took steps to address. In June 2010 the DHS IG reported that the U.S. Computer Emergency Readiness Team made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against cyber threats. However, the IG reported that the team could further improve its analysis and warning program. For example, the IG reported that the team could improve its management oversight by developing a strategic plan and establishing performance measures. Additionally, the IG reported that the team should improve its information sharing and communications coordination efforts with the public. Several factors have hampered DHS's ability to share information with its partners, including that threat information from intelligence agencies is classified. The DHS IG recommended, among other things, that DHS establish a consolidated, multiple classification level portal that can be accessed by federal partners that includes real-time incident response related information and reports. In addition, the DHS IG recommended the establishment of specific outcome-based performance measures and a strategic plan to ensure that the team can achieve its mission, objectives, and milestones. DHS concurred with these recommendations, and took action to implement them. For example, DHS reported that it established performance measures and a strategic plan, concept of operations, and standard operating procedures for the U.S. Computer Emergency Readiness Team. In July 2011 DHS also reported that it was taking steps to establish a multiple classification level portal.
Partnerships and coordination mechanisms	Federal partners, including DHS, developed new information-sharing arrangements, and DHS completed corrective actions based on a cybersecurity exercise. However, efforts to meet the expectations of private sector stakeholders in areas related to sharing information about cyber-based threats to critical infrastructure should be improved.	**DHS developed new information-sharing arrangements and completed corrective actions based on a cybersecurity exercise. However, additional action is needed to better ensure that expectations of private sector stakeholders are met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.** **Key progress:** DHS completed corrective actions based on lessons learned from a cybersecurity exercise. In September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing 8 lessons it had learned from this exercise to strengthen public and private incident response capabilities.[k] In the months following its first exercise, DHS identified 66 activities that address one or more of the lessons, including hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry, and refining their operating procedures. We reported in September 2008 that DHS's actions to address the lessons had not been fully implemented, and consequently recommended that DHS schedule and complete all of the corrective activities identified to strengthen coordination between public and private sector participants in response to significant cyber incidents. As of September 2010, DHS demonstrated that it had completed all 66 of the corrective actions addressing lessons learned from the exercise.

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: Federal policy, including DHS's *National Infrastructure Protection Plan*, calls for a partnership model that includes public and private councils to coordinate policy and information sharing and analysis centers to gather and disseminate information on threats to physical and cyber-related infrastructure.[l] In July 2010, we reported that while federal partners, such as DHS, were developing new information-sharing arrangements, they were not meeting the key expectations of the private sector. We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving private sector sharing of sensitive information. We recommended, among other things, that DHS use our findings to focus its information-sharing efforts on the most desired services, including access to sensitive or classified information and a secure mechanism for sharing information. DHS concurred with our recommendations and stated that it took steps to implement them, such as initiating pilot programs to enable the mutual sharing of cybersecurity information at various classification levels.[m] However, as DHS is initiating these pilot programs, it is too early to assess the extent to which they address the challenges we identified.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Sector specific agencies are lead federal agencies for the nation's critical infrastructure sectors, which include, for example, water and energy.

[b] At the time of our review, there were only 17 critical infrastructure sectors. DHS established the 18th sector—critical manufacturing—in March 2008 under the authority of the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.

[c] In addition, DHS reported that in 2009 it released the Information Technology Sector Baseline Risk Assessment and four associated risk management strategies, with it partner entities.

[d] The Trusted Internet Connection initiative is intended to improve security by reducing and consolidating external network access points and by providing centralized monitoring at a select group of access providers, while Einstein is an intrusion detection system that provides an automated process for DHS to analyze computer network traffic information to and from agencies.

[e] All federal agencies in the executive branch, except for the Department of Defense, have been directed to implement the initiative. The goals of the initiative are to secure federal agencies' external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network access points and implementing security controls over the access points that remain.

[f] Under the Trusted Internet Connections initiative federal agencies were required to (1) inventory external connections; (2) establish a target number of Trusted Internet Connections access points; (3) develop and implement plans to reduce their connections; (4) implement security capabilities (if they chose to be an access provider) addressing such issues as encryption and physical security; and (5) demonstrate to DHS the consolidation of connections and compliance with the security capabilities (if they chose to be an access provider).

[g] For example, the 16 agencies that chose to become access providers reported that they had reduced their number of external connections from 3,286 to approximately 1,753.

[h] In implementing the Trusted Internet Connections initiative, agencies could either provide their own access points by becoming an access provider or seek service from these providers or an approved vendor. For agencies seeking service, the agencies obtain services from a multi-service agency or through the Networx program. This program, managed by the General Services Administration, provides an acquisition vehicle for agencies to procure telecommunication, network, wireless, and information technology security services, including Trusted Internet Connections services, from among multiple vendors.

[i] We are conducting this work in accordance with a mandate in the Federal Information Security Management Act of 2002. Pub. L. No. 107-347, § 301(b), 116 Stat. 2946, 2953 (2002) (codified as amended at 44 U.S.C. § 3545(h)).

[j] According to DHS, in October 2009, it opened the new National Cybersecurity and Communications Integration Center—a 24-hour, DHS-led center to serve as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture; and, in November 2010, the Multi-State Information Sharing and Analysis Center, funded in part by DHS, opened the Cyber Security Operations Center, a 24-hour watch and warning facility, to enhance situational awareness at the state and local level and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments.

[k] These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

[l] Information-sharing and analysis centers were established to serve an operational role such as providing mechanisms for gathering, analyzing, and disseminating information on physical and cyber-related infrastructure threats and vulnerabilities to and from private infrastructure sectors and the government.

[m] DHS also reported that it participates in various working groups related to cybersecurity.

GAO Contact

For additional information about this area, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

Appendix XII: Emergency Preparedness and Response

What This Area Includes

Source: GAO.

U.S. 90 Bridge in Biloxi, Mississippi.

The Federal Emergency Management Agency (FEMA), within the Department of Homeland Security (DHS), is the federal agency primarily responsible for emergency preparedness and response efforts. FEMA's key responsibilities and efforts include national emergency preparedness and response planning, such as developing the *National Response Framework* and a national preparedness goal; providing emergency assistance and services, such as temporary housing assistance after a disaster; and supporting the federal government's state, local, and tribal partners' efforts to enhance their emergency management and homeland security capabilities, such as emergency communications, through grants and technical assistance.[1] As the primary component responsible for emergency preparedness and response, in fiscal year 2011 FEMA had approximately 7,300 personnel, and its budget authority was about $10.5 billion.[2] Emergency preparedness and response falls within the Quadrennial Homeland Security Review Mission 5: Ensuring Resilience to Disasters.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to emergency preparedness and response also include areas such as human capital management and training and exercise programs, we are not reporting on DHS's progress and work remaining in these areas. With regard to human capital, FEMA reported to us in July 2011 that it planned to increase its staffing levels to enhance FEMA's investigative operations and fraud awareness training initiatives by 50 percent in fiscal year 2011, and by another 50 percent in fiscal year 2012. We have not completed recent work on these areas upon which to make an assessment of DHS's progress.

[1]The National Response Framework is a guide for how the federal, state, local, and tribal governments, along with nongovernmental and private sector entities, will collectively respond to all disasters, ranging from large-scale terrorist attacks or catastrophic disasters such as Hurricane Katrina to serious local incidents, regardless of their cause. The national preparedness goal aims to define the core capabilities necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the United States, and emphasizes actions aimed at achieving an integrated, layered, and all-of-nation preparedness approach that optimizes the use of available resources.

[2] About $5.3 billion of this total was allocated to preparedness, disaster, and other grants, according to FEMA.

Key Progress and Work Remaining

Our work, supplemented by that of the DHS IG, has shown that FEMA expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; supported state, local, and tribal partners' disaster preparedness and response capabilities; and enhanced emergency communications. For example, FEMA developed various plans for disaster preparedness and response. In particular, FEMA issued the *National Response Framework*, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for disaster response. It 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. We also reported that FEMA awards certain preparedness grants based on a reasonable risk methodology. However, more work remains in FEMA's efforts to assess capabilities for all-hazards preparedness, provide long-term disaster recovery assistance, and strengthen alert systems. For example, FEMA has faced difficulties in collecting reliable and consistent data and developing measurable target capabilities for national preparedness. Further, with regard to long-term disaster recovery assistance, FEMA's criteria for when to provide the assistance were vague, and, in some cases, FEMA provided assistance before state and local governments had the capacity to work effectively with FEMA. Further, FEMA has faced technical challenges in implementing the Integrated Public Alert and Warning System related to systems integration and alerts for individuals with disabilities, among other things.[3] Additionally, FEMA should improve the efficacy of the grant application and review process by mitigating duplication or redundancy within the agency's various preparedness grant programs. Table 16 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[3] The Emergency Alert System is the nation's primary alerting system, proving capacity for the United States to issue alerts and warnings to the public in response to emergencies. The Integrated Public Alert and Warning System is defined by FEMA as a "system of systems," which is intended to integrate existing and new alert systems, including the Emergency Alert System. The Integrated Public Alert and Warning System will supersede the Emergency Alert System as the nation's primary alert function.

Table 16: Assessment of Progress and Work Remaining in Emergency Preparedness and Response on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
National emergency preparedness and response planning	DHS took steps to improve national emergency preparedness and response planning efforts by releasing the *National Response Framework* and strengthening response and recovery planning. However, a number of operational plans are not yet complete. Further, DHS has not developed measures for assessing national preparedness.	**FEMA issued the *National Response Framework* for disaster preparedness and response, but has not developed or implemented some plans and did not always ensure consistent stakeholder participation in the development and revision of all policies and plans.** **Key progress:** Planning and preparing for a major disaster—particularly a catastrophic disaster that could quickly overwhelm state and local responders—requires the coordinated effort of federal, state, local, and tribal governments, nongovernmental organizations, and the private sector, which owns much of the nation's critical infrastructure. In 2004 DHS issued the *National Response Plan*. In August 2005 Hurricane Katrina revealed a number of limitations in the 2004 *National Response Plan*, and DHS made modifications to it pending a more comprehensive review. DHS completed its revision with the issuance of the *National Response Framework* core document 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. In June 2008 we reported that during the revision process for the *National Response Framework*, DHS did not collaborate with non-federal stakeholders. For example, after the first draft of the *National Response Framework* was completed, DHS limited communication with non-federal stakeholders until it released another draft 5 months later. Further, DHS did not manage the revision process in accordance with the Post-Katrina Emergency Management Reform Act of 2006 provision that DHS establish FEMA's National Advisory Council and incorporate the Council's nonfederal input into the revision because the Council was created after the statutory target date and did not hold its first meeting until the final day of the public comment period for the *National Response Framework* draft.[a] Given that FEMA anticipates the Framework would be revised in the future, in June 2008 we recommended that FEMA develop policies and procedures to guide how future revision processes will occur, particularly for collaborating with nonfederal stakeholders. FEMA concurred and subsequently established provisions that direct the conditions and timing of revisions to the *National Response Framework*.[b] Further, in April 2009, we reported that FEMA had completed most of the key policies, such as the base *National Response Framework*, to define emergency preparedness and response roles and responsibilities. For example, DHS issued the revised National Incident Management System in December 2008 to further clarify roles and responsibilities when multiagency, intergovernmental entities are involved in a response.[c] FEMA also completed key components of the *National Response Framework*, including 15 Emergency Support Function Annexes, and 8 Support Annexes.[d]

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In April 2009 we reported that FEMA had not yet completed about two-thirds of the plans to operationalize the policies it had established to define emergency preparedness and response roles and responsibilities. As a result, the roles and responsibilities of key officials involved in responding to a catastrophe had not been fully defined and, thus, could not be tested in exercises. We recommended that FEMA establish a program management plan to ensure that the plans that were called for as part of the national preparedness system were developed in a timely and integrated fashion. FEMA generally concurred and has actions underway to address it. For example, FEMA told us that since we last reported, it has revised or completed six concept plans and approximately 28 hazard-specific regional plans. FEMA also reported working to implement elements of Presidential Policy Directive 8: National Preparedness. This directive instructs the Secretary of Homeland Security to develop a national preparedness goal and national preparedness system to meet that goal through an integrated set of guidance, programs, and processes. Specifically, FEMA reported in August 2011 that in response to Presidential Policy Directive 8, FEMA is leading the development of a Federal Interagency All-Hazards Response Plan, to include scenario-specific annexes that integrate prior earthquake, hurricane, and catastrophic planning efforts. To implement Presidential Policy Directive 8, FEMA will need to review its current and pending policies to ensure that they are consistent with the goals and requirements of the Directive, and make any adjustments that may be needed.
		Despite ongoing efforts to measure preparedness and assess capabilities, FEMA faced difficulties in collecting reliable and consistent data, and developing measurable target capabilities. **Key progress:** DHS, particularly FEMA, implemented efforts to measure preparedness by assessing capabilities and addressing related challenges. In September 2007, DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-based preparedness as a systematic effort that includes sequential steps to first determine capability requirements and then assess current capability levels. As a companion to the Guidelines, FEMA issued a Target Capabilities List, designed to provide a national-level generic model of capabilities defining all-hazards preparedness. FEMA also made progress in developing a system for assessing national preparedness capabilities by, among other things, establishing reporting guidance for state preparedness and issuing a federal preparedness report. Presidential Policy Directive 8, issued in March 2011, requires the development of a national preparedness goal, system, and report. The implementation plan for the directive calls for the development of the national preparedness goal by September 25, 2011, and the development of other documents by September 25, 2012.[e]

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: The success of FEMA's efforts to measure preparedness has been limited due to, among other things, missing quantifiable metrics to measure capabilities. In April 2009, we reported that establishing quantifiable metrics for target capabilities was a prerequisite to developing assessment data that can be compared across all levels of government. At the time of our review, FEMA was in the process of refining the target capabilities to make them more measurable and planned to develop quantifiable metrics for each of the capabilities. We reported in October 2010 that FEMA had not yet developed national preparedness capability requirements based on established metrics to provide a framework for assessing preparedness. FEMA officials told us that evaluation efforts that they used to collect data on national preparedness capabilities were useful for their respective purposes, but that the data collected were limited by data reliability and measurement issues related to the lack of standardization. Until a framework for assessing preparedness is in place, we reported that FEMA would 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. In our April 2009 report, we recommended that FEMA improve national preparedness by enhancing its project management plan for assessing capabilities to include reporting on the progress of preparedness assessments and developing quantifiable metrics for capabilities. DHS concurred, and in July 2011 FEMA reported that it took steps to establish a preparedness baseline and the accompanying foundation for assessing preparedness, including determining how effective grants are in improving preparedness. FEMA also reported that it was working with its emergency response partners to identify end-states, capabilities, and performance objectives for each emergency preparedness mission area as part of its development of the National Preparedness Goal. FEMA further will provide a summary of the progress being made towards developing and maintaining performance objectives required to deliver the capabilities described in the goal. In August 2011, FEMA reported that it had established a Program Executive Office to ensure that the target dates for implementation of Presidential Policy Directive 8 are met and stakeholders are engaged in the process. As these efforts are recent, we have not conducted work to assess their effectiveness in measuring preparedness. However, in the past FEMA has had difficulty meeting target dates, thus it will be important for FEMA to effectively consult with and incorporate the input of its many stakeholders to support meeting this schedule.

Area	Overall assessment	Summary of key progress and work remaining
		DHS and FEMA have strengthened nationwide recovery planning efforts, but efforts are in the early stages. **Key progress:** In February 2010, FEMA released a draft National Disaster Recovery Framework, which is intended to provide a model to collectively identify and address challenges that arise during the disaster recovery process. This Framework is designed to help the emergency management community work better together to support individuals, households, and communities as they rebuild and restore their ways of life following a disaster. FEMA later reported that since March 2010, it has received hundreds of comments and recommendations from federal agencies and departments on the proposed Framework. In March 2010, we reported that FEMA assisted local communities with developing long-term disaster recovery plans as part of its post-disaster assistance. For example, one way FEMA 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. Local officials credited this assistance with helping the city to be able to secure federal funding. **What remains to be done:** We have identified areas where FEMA's recovery assistance to local communities should be improved. For example, state and local officials in Texas recovering from Hurricane Ike in 2008 said that FEMA's process of ranking projects in the City of Galveston's recovery plan had the effect of fostering unrealistic expectations among the public about what projects would be funded. We recommended that FEMA more clearly communicate the objectives and processes it uses when assessing the value of specific recovery projects to help prevent unrealistic expectations about the implementation of such projects among members of the affected community. DHS agreed and stated that it would further examine the tools it used to communicate with impacted communities as part of the implementation of the National Disaster Recovery Framework. With regard to Framework, in July 2011, FEMA reported that the revised draft of the Framework was in the final stages of interagency review and interagency teams had been working to develop draft annexes for the six core functional areas of the Framework. Since FEMA has not yet finalized this framework, it is too early to assess its results.
Provision of emergency assistance and services	FEMA improved emergency assistance services and oversight of disaster-related emergency assistance, but should further strengthen its management of emergency response and recovery assistance programs.	**FEMA improved the provision and oversight of emergency assistance and services, but work remains in its management and operation of emergency response and recovery assistance programs.** **Key progress:** FEMA has provided and coordinated the provision of assistance to state and local governments, non-profit organizations, and individuals after disasters—-including helping communities develop long-term recovery plans. In June 2011, the DHS IG reported that it had identified 128 programs that provide disaster assistance and that DHS administers 69, or approximately 54 percent, of these programs. For example, FEMA operates the Public Assistance program, which provides grants to state, local, and tribal governments and certain non-profit organizations.

Area	Overall assessment	Summary of key progress and work remaining
		FEMA also took steps to improve its disaster assistance program oversight. In December 2008, we identified challenges in the Public Assistance program related to project development, information sharing and tracking the status of projects, project approvals and appeals, and human capital. For example, disagreements between applicants and FEMA, as well as changes to project scope decisions, contributed to slowing down project development. We reported that DHS had addressed these challenges, including finalizing a public assistance catastrophic disaster recovery concept plan that recognized the need to more easily tailor projects to meet post-disaster conditions; developing new management information systems to better track and manage projects and increase the transparency of public assistance funding; and creating a credentialing program for employees. Further, in July 2011, FEMA reported that it had established two Public Assistance review panels within the Public Assistance appeals process for the purpose of expediting final eligibility decisions for disputed projects. With respect to employee credentialing, FEMA reported in July 2011 that its newly created FEMA Qualification System is intended to build upon previous efforts to credential FEMA's disaster response personnel. According to FEMA, the system is expected to improve workforce qualification and certification of FEMA personnel deployed for incident management and support operations. We are conducting ongoing work related to FEMA's disaster assistance workforce and plan to report on our results in 2012.[f] **What remains to be done:** In March 2010, we identified two broad challenges related to FEMA's long-term disaster recovery assistance efforts. First, the criteria for when FEMA was to provide long-term recovery assistance in a specific disaster were vague, which resulted in uncertainty among other federal agencies and state recovery officials. Second, in some cases, FEMA assistance began before state and local governments had the capacity to effectively work with FEMA and ended before critical long-term recovery coordination and planning needs were fully addressed. We recommended, among other things, that DHS develop clear and consistent criteria that identify factors that determine whether and how the entity responsible for coordinating long-term recovery will become involved in a specific disaster. We also recommended that DHS establish a long-term recovery structure that more effectively aligns the timing and level of involvement of the entity responsible for coordinating long-term community recovery assistance with both the capacity of state and local governments to work with them and the need for coordination assistance. DHS concurred and reported in July 2011 that it had developed an assessment tool to assist a coordinating officer or state when attempting to determine if activating the long term recovery mission is appropriate. These are positive steps that should help strengthen FEMA's efforts to address timing issues with its disaster recovery, but they are still in the early stages of implementation.

Area	Overall assessment	Summary of key progress and work remaining
		Additionally, FEMA reported in July 2011 that it sought to increase its disaster reservist cadre with professionals in areas of community planning, city management, and economic recovery to also provide an enhanced technical resource to local governments early in recovery efforts to assist in launching recovery planning. These are positive steps that should assist FEMA in its recovery efforts. However, because of the long-term nature of disaster recovery, it will take time to determine the impact of these efforts in enhancing recovery from such recent disasters as the tornados that devastated areas of Alabama and Missouri.
Emergency and interoperable communications	DHS and FEMA made strategic progress in enhancing emergency and interoperable communications. However, specific alert systems, such as the Integrated Public Alert and Warning System, have technical challenges, such as message delivery limitations.	**DHS and FEMA released key emergency communications strategic documents and made grants available for interoperability, but have made limited progress to enhance emergency alert systems.** **Key progress:** Continuity of communications, capacity, and interoperability are primary areas of vulnerability in emergency communications. Emergency communications breakdowns undermined response efforts during terrorist attacks in 2001 and Hurricane Katrina in 2005. In response, federal agencies, including DHS, increased efforts to enhance emergency communications. In June 2009, we reported that DHS and other federal agencies took steps to enhance emergency communications by issuing key documents such as the *National Emergency Communications Plan*—the first strategic document for improving emergency communications nationwide. Further, DHS and other federal agencies made numerous grants for interoperable communications available and increasingly aligned them with national and state plans. In addition, we reported that federal agencies, including DHS, took strategic steps to assist first responders. In March 2010, we reported that the Emergency Communications Preparedness Center had been established. At that time, the members were developing a working definition of the scope of emergency communications to define the scope of their mission and the types of information that should be included in an emergency communications clearinghouse. As of July 2011, DHS reported that the membership of the Preparedness Center expanded to 14 federal agencies, and the members had developed strategic objectives and an action plan to implement these objectives. FEMA also reported that it established and implemented working groups and a Disaster Emergency Communications Division to support emergency and interoperable communications.

Area	Overall assessment	Summary of key progress and work remaining
		Further, in September 2009, we reported on the Emergency Alert System, the primary national-level public warning system, and FEMA's Integrated Public Alert and Warning System, which is intended to integrate new and existing alert capabilities, including the Emergency Alert System, into a "system of systems" to become the country's comprehensive public alert system. We reported that FEMA faced coordination issues in developing and implementing the system. For example, many stakeholders we contacted during our work knew little about the Integrated Public Alert and Warning System and expressed the need for better coordination with FEMA. Among other things, we recommended that FEMA develop strategic goals and processes for deployment of the Integrated Public Alert and Warning System and report periodically on program progress to the Congress and to the Secretary of Homeland Security in order to improve program transparency and accountability. DHS concurred and published an Integrated Public Alert and Warning System Strategic Plan in June 2010 that identified the vision, mission, goals and objectives of the program.[g] **What remains to be done:** In September 2009, we reported that FEMA faced technical challenges in implementing the Integrated Public Alert and Warning System related to systems integration, standards development, the development of geo-targeted and multilingual alerts, and alerts for individuals with disabilities. For example, FEMA's standard intended to facilitate integration of alert systems was under development and not widely used. As a result, we reported that integration with state and local systems would likely be a significant challenge due to potential incompatibility, and FEMA did not yet have logistical plans to integrate these systems. Further, we reported that to demonstrate the integration and expansion of new alerting technologies, and to work toward the functionality described in the executive order, FEMA had implemented pilot projects, but they ended inconclusively, with few documented lessons learned. We recommended, among other things, that FEMA establish and implement a plan to verify the dependability and effectiveness of systems used to disseminate alerts. FEMA concurred and, in July 2011, reported that it had engaged with a range of agencies, organizations, and private sector entities to promote Integrated Public Alert and Warning System capabilities and opportunities for the integration of alert and warning technologies for people with access and functional needs. FEMA reported that it had partnered with organizations to demonstrate products that incorporate technologies for alerting persons with access and functional needs. Further, FEMA reported that it was developing an infrastructure of alert and warning capabilities that expands on the traditional Emergency Alert System by, for example, allowing individuals with enabled mobile devices to receive text-like messages alerting them of imminent threats in their geographic area. FEMA reported that in March 2011 it deployed the Integrated Public Alert and Warning System-Open Platform for Emergency Networks, a set of securely hosted Web services that enable the routing of alerts and warnings between various third-party systems, networks, and devices. As DHS has recently implemented this system and its pilot products have not yet been deployed, it is too early to assess the effectiveness of these efforts.

Area	Overall assessment	Summary of key progress and work remaining
Support to state and local partners	FEMA made progress in allocating homeland security grants using a reasonable risk assessment methodology. However, challenges remain regarding the coordination of grant programs.	**FEMA used a reasonable risk assessment methodology to allocate the Urban Areas Security Initiative and State Homeland Security grants, but FEMA should coordinate the application and review process for its preparedness grants.** **Key progress:** Within FEMA, the Grant Programs Directorate is responsible for business operations, training, policy, oversight of all FEMA grants, and the program management of preparedness grants. FEMA's grant programs vary from enhancing capabilities that focus on counterterrorism and catastrophic events, to specific first-responder disciplines that strengthen capabilities for addressing hazards of all types. For example, the State Homeland Security Program provides funding in an effort to address the identified planning, organization, equipment, training, and exercise needs at the state and local levels to prevent, protect against, respond to, and recover from acts of terrorism and other catastrophic events. The Urban Areas Security Initiative program provides funding to address the unique planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. In June 2008, we reported that DHS had constructed a reasonable methodology to assess risk and allocate the Urban Area Security Initiative and State Homeland Security grants, but that this methodology did not account for vulnerability differences among jurisdictions. In July 2011, DHS reported that it modified its methodology for fiscal year 2011 to address the measurement of vulnerability in its risk-based grant allocation model. Specifically, FEMA reported creating a separate vulnerability assessment that accounts for 20 percent of the overall risk assessment for states, and territories, and the top 100 metropolitan areas for use in the State Homeland Grant Program and the Urban Areas Security Initiative grant program. We have ongoing work assessing these homeland security grant programs, and plan to report on the results later this year.[h] **What remains to be done:** In March 2011 we reported that until FEMA evaluates grant applications across grant programs, FEMA cannot ascertain whether or to what extent multiple funding requests are being submitted for similar purposes. In March 2010, the DHS IG reported that FEMA should improve the efficacy of the grant application and review process by taking steps to mitigate duplication or redundancy within the agency's various preparedness grant programs. Specifically, the DHS IG found that FEMA's grant application process risked being ineffective because it did not compare and coordinate grant applications across programs to identify and mitigate potential duplications. Additionally, grant application processes were not efficient, requiring FEMA and state and local grant administrators to expend time and resources fulfilling redundant requirements for the numerous grant programs.

Area	Overall assessment	Summary of key progress and work remaining
		The IG recommended, among other things, that FEMA identify grant programs that may overlap or duplicate with other programs. FEMA concurred and reported it planned to take action to address them. For example, FEMA reported in July 2011 that it was working with DHS and other federal departments to consolidate existing preparedness grant programs and entering into a memorandum of understanding with the Departments of Health and Human Services and Transportation to clarify roles among the departments regarding their emergency preparedness-related grants. These are positive steps and should help strengthen FEMA's grant management. However, our work and that of the DHS IG has shown that FEMA should further benefit from examining its grant programs and coordinating its application process to eliminate or reduce redundancy among grant recipients and program purposes.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] The Post-Katrina Emergency Management Reform Act required the Secretary of Homeland Security to establish a National Advisory Council to advise the FEMA Administrator on all aspects of emergency management. Among its specific responsibilities, the Council was to incorporate input from state, local, and tribal governments as well as the private sector in the development and revision of the 2004 *National Response Plan*. 6 U.S.C. § 318.

[b] In July 2011, FEMA reported that it had begun using a "Whole Community" approach in which it was engaging non-federal stakeholders in its preparedness planning efforts. For example, FEMA reported that, in implementing elements of Presidential Policy Directive 8, which was issued on March 30, 2011, it had engaged non-federal stakeholders, such as the National Advisory Council, the Local, State, Tribal and Federal Preparedness Task Force and state and local associations. FEMA also reported taking steps to increase private sector participation by, among other things, creating a private sector division to increase coordination during disaster planning, response and recovery efforts, such as National Level Exercise 2011, establishing a seat for a private sector representative to work with FEMA and other federal partners at the National Response Coordination Center, and planning to incorporate private sector and nongovernmental representatives to participate in response and recovery exercises.

[c] The National Incident Management System presents, among other things, doctrine that standardizes the process for emergency response stakeholders to conduct integrated emergency management and incident response operations by establishing organizational incident management structures.

[d] The *National Response Framework* Emergency Support Function Annexes align categories of federal government response resources and capabilities and provide strategic objectives for their use under the *National Response Framework*. The *National Response Framework* Support Annexes describe the roles and responsibilities of federal departments and agencies and nonfederal entities in coordinating and executing the common functional processes and administrative requirements necessary for incident management that are common to all incidents.

[e] The implementation plan for Presidential Policy Directive 8 includes target dates for the first edition of a national preparedness goal (September 25, 2011), a document describing the national preparedness system (November 24, 2011), the first national preparedness report (March 30, 2012), the first edition of the national planning frameworks (June 30, 2012) and the first edition of the interagency operational plans to support the delivery of capabilities in each of the frameworks (September 25, 2012).

[f] We are conducting this review at the request of the House Committee on Homeland Security and the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Senate Committee on Homeland Security and Governmental Affairs and plan to report on the results of our review in 2012.

[g] Federal Emergency Management Agency. *Strategic Plan for the Integrated Public Alert and Warning System (IPAWS) Program.* June 2010.

[h] We are conducting this work for the House Committee on Homeland Security; the Senate Committee on Homeland Security and Governmental Affairs; and the Senate Committee on Commerce, Science, and Transportation.

GAO Contacts

For additional information about this area, contact William O. Jenkins, Jr. at (202) 512-8757 or jenkinswo@gao.gov.

Appendix XIII: Department of Homeland Security Transformation and Implementation

What This Area Includes

In 2003, we designated implementing and transforming the Department of Homeland Security (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. This high-risk area includes challenges in strengthening DHS's management functions, the impact of those challenges on DHS's mission implementation, and challenges in integrating management functions within and across the department and its components.[1]

For the purposes of this report, we are highlighting examples of DHS transformation and implementation efforts in key areas on which we have recently reported, and not on areas on which we have not reported or have conducted limited audit work. DHS has other transformation and implementation efforts underway at the department and component levels. We have not completed work on these areas upon which to base an assessment of DHS's progress.

Key Progress and Work Remaining

DHS took action to strengthen and integrate its acquisition, information technology, financial, and human capital management functions. However, further action is needed to address management challenges, which have hindered DHS's efforts to implement its missions by, for example, contributing to program delays and performance problems.

DHS has strengthened its management functions. For example, the department revised its acquisition management oversight policies to include more detailed guidance to inform departmental acquisition decision making. DHS also developed corrective action plans for financial management weaknesses, and the number of conditions contributing to departmentwide material weaknesses has declined at the component level since 2005.[2] Further, DHS issued its *Workforce Strategy for Fiscal Years 2011-2016* in December 2010, which contains the department's

[1] We define management integration as the development of consistent and consolidated processes, systems, and people—in areas such as information technology, financial management, procurement, and human capital—as well as in its security and administrative services, for greater efficiency and effectiveness.

[2] A material weakness is a significant deficiency, or a combination of significant deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

workforce goals, objectives, and performance measures for human capital management. However, DHS continues to face significant weaknesses in these areas that hinder the department's transformation efforts and its ability to meet its missions. For example, because of acquisition and information technology management weaknesses, major programs have not met capability, benefit, cost, and schedule expectations. Further, we reported that financial management internal control weaknesses have impeded DHS from providing reliable and timely financial data to support daily operational decision making. Moreover, human capital challenges have affected departmental and component efforts to implement their missions. As DHS continues to mature as an organization, it will be critical that the department continue to work to strengthen its management functions and their implementation, since the effectiveness of these functions and their implementation directly affects its ability to fulfill its homeland security and other missions.

DHS has developed and begun to implement its strategy to address the high-risk area, but has not yet demonstrated sustainable, measurable progress in its implementation efforts. In our 2011 high-risk update, we reported that DHS has taken action to implement, transform, and strengthen its management functions. The Secretary and Deputy Secretary of Homeland Security, and other senior officials, have demonstrated commitment and top leadership support to address the department's management challenges. In January 2011, DHS provided us with its *Integrated Strategy for High Risk Management*, which summarized the department's preliminary plans for addressing the high-risk area, and DHS updated this strategy in June 2011. We provided DHS with feedback on the January 2011 strategy and have worked with the department to monitor implementation efforts. For example, we noted that the January 2011 strategy was generally responsive to actions and outcomes we identified for the department to address the high-risk area. However, we noted that, in most cases, the strategy did not identify the specific resources needed to implement planned corrective actions, making it difficult to assess the extent to which DHS has the capacity to implement these actions. Additionally, we noted that the strategy did not provide information on the underlying metrics or factors DHS used to rate its progress, making it difficult for us to assess DHS's overall characterizations of progress. In the June 2011 update, DHS provided ratings of its progress in implementing corrective actions related to each management function. We are assessing DHS's ratings and the June 2011 update, and plan to provide the department with our feedback later this year.

Going forward, to address the long-standing problems in its management functions and in the integration of those functions, DHS needs to implement its *Integrated Strategy for High Risk Management*; continue its efforts to identify and acquire resources needed to achieve key actions and outcomes; implement a program to monitor and validate its corrective actions; and show measurable, sustainable progress in implementing corrective actions and achieving key outcomes.

DHS developed processes and policies for managing its acquisitions, but faces significant challenges in ensuring proper implementation. DHS has taken steps to strengthen acquisition oversight processes, but it continues to face obstacles in managing its acquisitions and ensuring proper implementation and departmentwide coordination. We previously reported that DHS faced challenges related to acquisition oversight, cost growth, and schedule delays. In August 2007, DHS established the Acquisition Program Management Division under the Office of the Chief Procurement Officer to help strengthen acquisition management within the department. Further, in June 2010, we reported that DHS continued to develop its acquisition oversight function and had begun to implement a revised acquisition management directive that includes more detailed guidance for programs to use when informing component and departmental decision making. We also reported that the senior-level Acquisition Review Board had met more frequently and provided programs decision memorandums with action items to improve performance.[3] However, while the Acquisition Review Board reviewed 24 major acquisition programs in fiscal years 2008 and 2009, more than 40 major acquisition programs had not been reviewed, and programs had not consistently implemented action items identified as part of the review by established deadlines. In July 2011, DHS reported that the Acquisition Program Management Division in 2009 started conducting annual portfolio program reviews with components with the goal of ensuring that major programs receive at least one review on an annual basis, and that DHS had conducted reviews of additional programs through the Acquisition Review Board in fiscal years 2010 and 2011.

[3] The Acquisition Review Board is the DHS executive board that reviews major acquisition programs. Among other things, the board reviews select acquisitions for executable business strategy, resources, management, accountability, and alignment to strategic initiatives. It also approves acquisitions to proceed to their next acquisition life-cycle phases upon satisfaction of applicable criteria.

Our work has also shown that departmental concerns exist about the accuracy of cost estimates for some of DHS's major programs.[4] In addition, over half of the programs we reviewed for our June 2010 report awarded contracts to initiate acquisition activities without component or department approval of documents essential to planning acquisitions, such as mission need statements outlining the specific functional capabilities required to accomplish DHS's mission and objectives; operational requirements; and acquisition program baselines. Additionally, in November 2010, leveraging our work, the DHS Office of Inspector General (IG) identified acquisition management as a major challenge facing the department. We have made a number of recommendations to DHS to strengthen its acquisition management functions, such as establishing a departmental joint requirements oversight board to review and approve acquisition requirements, and ensuring major investments comply with established component and departmental review policy standards. DHS generally agreed and is working to address them by, among other things, establishing an Investment Review Board to help oversee the status of all acquisition investments; expanding its Acquisition Corps to provide trained procurement and program management professionals to manage DHS's most critical acquisition programs; developing a tool to track programs' cost, schedule, and performance indicators; and evaluating the effectiveness of award fees and performance incentives. These are positive actions that should better position DHS to meet its acquisition needs. However, moving forward, DHS will need to continue to demonstrate sustainable progress in implementing these actions and delivering programs that meet cost, schedule, and performance expectations.

DHS established information technology management controls, capabilities, and policies, but gaps remain in implementing management policies and procedures. DHS established information technology management controls and capabilities, but in September 2009 we reported that DHS made uneven progress in its information technology management efforts to institutionalize a framework of

[4] In June 2008, DHS established the Cost Analysis Division to help validate cost estimates. In July 2011, DHS reported that it plans to combine this division with the Acquisition Program Management Division to create a new office—tentatively called the Office of Program Accountability and Risk Management—to report directly to the Under Secretary for Management.

interrelated management controls and capabilities. For example, DHS continued to issue annual updates to its enterprise architecture that added previously missing scope and depth, and further improvements were planned to incorporate the level of content, referred to as segment architectures, needed to effectively introduce new systems and modify existing ones.[5] In addition, in July 2011, DHS reported that the department had begun tracking implementation of our Enterprise Architecture Management Maturity Framework and had developed plans to improve enterprise architecture maturity within each component and departmentwide.[6] We further reported that DHS redefined its information technology acquisition and investment management policies, practices, and structures, including establishing a system life cycle management methodology, and increased its information technology acquisition workforce.[7] In addition, in August 2011, DHS reported that it had efforts underway to establish an information technology program manager certification track intended to assist in managing information technology program management challenges.

Nevertheless, challenges remain relative to, for example, fully defining key system investment and acquisition management policies and procedures for information technology. Moreover, the extent to which DHS implemented these investment and acquisition management policies and practices on major information technology programs has been inconsistent. For example, our work showed that major information technology acquisition programs were not subjected to executive-level acquisition and investment management reviews. As a result, major programs aimed at delivering important mission capabilities had not lived up to their capability, benefit, cost, and schedule expectations.

We also reported on challenges departments, including DHS, have faced in implementing controls to protect their computer systems and networks. For example, we reported on the need for federal agencies, including DHS, to improve implementation of information security controls, such as

[5] Enterprise architecture is a corporate blueprint that serves as an authoritative frame of reference for information technology investment decision making.

[6] Our Enterprise Architecture Management Maturity Framework provides a practical approach for incrementally developing and implementing an enterprise architecture.

[7] A system life cycle management process normally begins with initial concept development and continues through requirements definition to design, development, various phases of testing, implementation, and maintenance.

those for configuring desktop computers and wireless communication devices. Additionally, in November 2010, the DHS IG identified information technology management as a major challenge facing the department. For example, the DHS IG reported that the department faces challenges as it attempts to create a unified information technology infrastructure for effective integration and agencywide management of information technology assets and programs. We made recommendations to strengthen DHS information technology management, such as establishing procedures for implementing project-specific investment management policies, and policies and procedures for portfolio-based investment management. DHS is working to strengthen these areas by, for example, developing a process for information technology acquisition management to help ensure that each investment begins with a successful plan and road map for its life cycle and by establishing executive steering committees to monitor the cost and schedule performance of all high-risk information technology investments. While these are positive steps that should better position the department in managing its information technology investments moving forward, DHS will need to continue to make measurable progress in implementing these actions and successfully developing and deploying information technology programs.

DHS took steps to address financial management weaknesses, but faces challenges in modernizing its financial systems and has been unable to obtain an unqualified audit opinion. DHS made progress in addressing its financial management and internal controls weaknesses. For example, DHS reduced the number of conditions at the component level contributing to departmentwide material weaknesses since 2005. However, DHS twice attempted to implement an integrated departmentwide financial management system, but has not been able to

consolidate its disparate systems.[8] In addition, DHS has not been able to obtain an unqualified audit opinion on its consolidated financial statements (i.e., prepare a set of financial statements that are considered reliable). For fiscal year 2010, the independent auditor issued a disclaimer on DHS's consolidated financial statements and identified deficiencies in DHS's internal control over financial reporting. Until these weaknesses are resolved, DHS will not be in position to provide reliable, timely, and useful financial data to support day-to-day decision making. In addition, as a result of these weaknesses, in November 2010 the DHS IG assessed financial management as one of the major management challenges facing the department. DHS has taken steps to prepare and implement corrective action plans for its internal control weaknesses through its *Internal Control Playbook*, DHS's annual plan to design and implement departmentwide internal controls. Further, in fiscal year 2010 DHS committed to the goal of receiving a qualified audit opinion on its consolidated balance sheet in fiscal year 2011, and the department is working toward that goal by, for example, focusing on strengthening budgetary resource processes and payment management, and remediating financial management issues at the U.S. Coast Guard. These are positive first steps toward achieving a successful full scope audit of the department's consolidated financial statements and, if implemented effectively, should help DHS strengthen its financial management functions.

DHS issued plans for human capital activities, but has not yet fully addressed barriers to equal opportunity employment and assessed foreign language workforce needs and gaps. DHS issued various strategies and plans for its human capital activities and functions. For example, in December 2010 DHS issued its *Workforce Strategy for Fiscal Years 2011-2016,* which contains the department's workforce goals,

[8] Since its creation, DHS has made two attempts to implement an integrated departmentwide financial management system—first through its Electronic Managing Enterprise Resources for Government Efficiency and Effectiveness program and second through its Transformation and Systems Consolidation program. As we reported in June 2007, DHS had ended its Electronic Managing Enterprise Resources for Government Effectiveness and Efficiency effort after determining that the resulting financial management systems would not provide the expected system functionality and performance. In December 2009, we reported that the Transformation and Systems Consolidation program had been affected by bid protests and related litigation which was contributing to a significant delay in awarding a contract. DHS ended this program in May 2011 and reported that moving forward it would consider alternatives to meet revised requirements.

objectives, and performance measures for human capital management. These strategies are promising, but DHS has faced challenges in implementing its human capital functions, including hiring people with the needed skills and abilities in areas such as acquisition management, for example. Further, our prior work suggests that successful organizations empower and involve their employees to gain insights about operations from a frontline perspective, increase their understanding and acceptance of organizational goals and objectives, and improve motivation and morale. However, DHS's scores on the Partnership for Public Service's 2010 rankings of the Best Places to Work in the Federal Government improved from prior years, but in 2010, it was ranked 28 out of 32 agencies in the Best Places to Work ranking on overall scores for employee satisfaction and commitment.[9]

In addition, our prior work identified several workforce barriers to achieving equal employment opportunities and the identification of foreign language needs and capabilities at DHS. In August 2009 we reported that DHS developed a diversity council, among other initiatives, but that DHS generally relied on workforce data and had not regularly included employee input from available sources to identify triggers to barriers to equal employment opportunities, such as promotion and separation rates. In June 2010 we reported on DHS's foreign language capabilities, noting that DHS took limited actions to assess its foreign language needs and existing capabilities and to identify potential shortfalls.[10] Assessing hiring needs is crucial in achieving a range of component and departmentwide missions. We recommended that DHS incorporate employee input in identifying potential barriers to equal employment opportunities and comprehensively assess its foreign language needs and capabilities. DHS concurred and reported having actions underway to address the recommendations, such as launching an exit survey across DHS in fiscal year 2011 to help use employee input to identify equal employment opportunity barriers, developing a task force to identify foreign language requirements, completing two foreign language assessments departmentwide, and planning to establish a language services executive

[9] Partnership for Public Service and the Institute for the Study of Public Policy Implementation at the American University School of Public Affairs, *The Best Places to Work in the Federal Government* (Washington, D.C.: 2010).

[10] DHS has a variety of responsibilities that utilize foreign language capabilities, including investigating transnational criminal activity and staffing ports of entry into the United States.

steering committee to provide oversight of the department's language requirements. DHS reported that it is also working to address its human capital management challenges by, among other things, developing component operational plans for the *Workforce Strategy,* tracking those plans against a common set of performance measures, and implementing comprehensive workforce planning to link the department's strategic goals, mission critical occupations, and workforce capacity and capabilities. These are positive actions that should better position DHS in assessing and meeting its human capital needs, but more work remains.

DHS took action to integrate its management functions, but needs to continue to demonstrate sustainable progress in integrating those functions within and across the department and its components. DHS took action to integrate its management functions. For example, DHS put in place common policies, procedures, and systems within individual management functions, such as human capital, that help to integrate its component agencies. In November 2009, we reported that DHS had not yet developed a strategy for management integration with characteristics we recommended, such as clearly identifying critical links that must occur among management initiatives and identifying potential efficiencies. In the January 2011 *Integrated Strategy for High Risk Management,* as well as the June 2011 update, DHS included a management integration plan containing information on ongoing and planned initiatives to integrate its management functions within and across the department and its components. For example, DHS plans to establish a framework for managing investments across its components and management functions to strengthen integration within and across those functions, as well as to ensure mission needs drive investment decisions. This framework seeks to enhance DHS resource decision making and oversight by creating new department-level councils to identify priorities and capability gaps, revising how DHS components and lines of business manage acquisition programs, and developing a common framework for monitoring and assessing implementation of investment decisions. These actions, if implemented effectively, should help to further and more effectively integrate the department. We also reported that DHS needs to continue to implement corrective actions within individual management areas, such as acquisition and financial management, to develop consistent or consolidated processes and systems within and across the department and its components. DHS is working to implement these corrective actions which, if implemented effectively, should help DHS drive integration of its management functions. Going forward, we will continue to review and provide feedback

on DHS's updated plan for management integration and will monitor implementation efforts.

GAO Contacts

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov for transformation, human capital management, and management integration; John Hutton at (202) 512-4841 or huttonj@gao.gov for acquisition management; David A. Powner at (202) 512-9286 or pownerd@gao.gov for information technology management; or Paula Rascona at (202) 512-9816 or rasconap@gao.gov for financial management.

Appendix XIV: Performance Measurement

What This Area Includes

Performance measurement underpins federal efforts to assess and report on progress in strengthening programs and operations. We reported on the importance of the development of outcome-based performance goals and measures as part of results management efforts across government. Performance goals and measures are intended to provide Congress and agency management with information to systematically assess a program's strengths, weaknesses, and performance. A performance goal is the target level of performance expressed as a tangible, measurable objective against which actual achievement will be compared. A performance measure can be defined as an indicator, statistic, or metric used to gauge program performance. Outcome-oriented measures show results or outcomes related to an initiative or program in terms of its effectiveness, efficiency, or impact.

For the purposes of this report, we are generally highlighting examples of Department of Homeland Security (DHS) performance measurement efforts in key areas on which we have recently reported, and not on areas on which we have not reported or have conducted limited audit work. DHS has other performance measurement efforts underway at the department and component levels. We have not completed work on these areas upon which to base an assessment of DHS's progress.

Key Progress and Work Remaining

DHS has strengthened its performance measures in recent years and has linked its measures to the Quadrennial Homeland Security Review's (QHSR) missions and goals. However, DHS and its components have not yet fully developed measures for assessing the effectiveness of some key homeland security programs, such as programs for securing the border, enforcing immigration laws, and preparing the nation for emergency incidents.

DHS has strengthened its performance measures, but has not yet fully developed outcome-based measures for assessing progress and performance for many of its mission functions. Over the past 3 years, DHS has strengthened its performance measures. In 2007, we reported on progress made by DHS in implementing its mission and management functions by assessing actions taken by DHS to achieve performance expectations set for the department in legislation, presidential directives, and DHS and component strategic plans and documents.[1] We noted that DHS generally had not established 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 these expectations. At the request of the Senate Committee on Homeland Security and Governmental Affairs following the issuance of that report, we provided DHS with feedback on the

[1] The performance expectations we identified for DHS in this report do not represent performance goals or measures for the department.

department's performance goals and measures to help strengthen DHS's efforts in this area. Our feedback was based on our work on and subject matter knowledge of the programs, activities, and areas being measured, as well as our work on effective practices for performance measurement. This feedback ranged from pointing out components' limited use of outcome-oriented performance measures to assess the results or effectiveness of programs, to raising questions about the steps DHS or its components took to ensure the reliability and verification of performance data. DHS also implemented internal efforts to strengthen its performance measures. For example, as part of our ongoing review of the QHSR, we found that DHS worked to align its performance measures to the QHSR missions and goals.[2] The department also provided components with guidance that outlines how to assess QHSR missions and related training, and formed working groups to discuss implementing specific performance measure concepts. Further, DHS reported that after the QHSR was issued, DHS senior leaders held meetings to discuss how to revise existing performance measures, and components worked to develop improved performance measures.

In response to its internal efforts and our feedback, DHS developed and revised its performance goals and measures for some areas to strengthen its ability to assess its outcomes and progress. For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its QHSR missions and goals. In addition to these strategic measures, the department has 132 management measures, which DHS uses for assessing programmatic performance and for resource allocation and other internal decision making purposes, such as program evaluation. In addition, in July 2011, DHS reported that the department has identified 24 areas for focused efforts to develop enhanced measures, based on guidance from DHS leadership and the Office of Management and Budget. These areas address gaps in both strategic and management measures for specific mission areas. DHS also plans to continue its annual process for reviewing and working to strengthen its performance measures.

While DHS has made progress in strengthening performance measurement, our work across the department has shown that a number

[2] We are conducting this review at the request of the Senate Committee on Homeland Security and Governmental Affairs and plan to report on our results later this year.

of programs lack outcome goals and measures, which may hinder the department's ability to effectively assess results or fully assess whether the department is using resources effectively and efficiently. We have recognized that DHS faces some inherent difficulties in developing performance goals and measures to address its unique mission and programs, such as in developing measures for the effectiveness of its efforts to prevent and deter terrorist attacks. In such instances, proxy measures—or indirect indicators—should be designed to assess the effectiveness of program functions. Outcome measures are helpful to departmental decision makers and managers, as they describe the products and services delivered by a program over a period of time. However, we have reported that many of DHS's components have not developed adequate proxy or outcome-based performance measures or mechanisms to monitor, assess, and evaluate the effectiveness of their plans and performance. Such measures, along with output and process measures, would help DHS track progress being made toward specific goals and provide managers with important information upon which to base their decisions.

Our work has shown that DHS and its components did not have performance measures for assessing the effectiveness of key border security and immigration programs. For example, in September 2009 we reported that U.S. Customs and Border Protection (CBP) had invested $2.4 billion in tactical infrastructure (fencing, roads, and lighting) along the southwest border under the Secure Border Initiative—a multiyear, multibillion dollar program aimed at securing U.S. borders and reducing illegal immigration. However, DHS could not measure the impact of this investment in tactical infrastructure on border security. We recommended that DHS conduct an evaluation of the impact of tactical infrastructure on effective control of the border. DHS concurred and reported considering using independent researchers for evaluations. We also reported in August 2009 that CBP had established three performance measures to report the results of checkpoint operations, which provided some insight into checkpoint activity.[3] 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. We recommended that CBP

[3] CBP operates checkpoints on U.S. roads, mainly in Southwest border states, at which agents screen vehicles for unauthorized aliens and contraband.

improve the measurement and reporting of checkpoint effectiveness. CBP agreed and reported plans to develop and better use data on checkpoint effectiveness.

Further, we reported that U.S. Immigration and Customs Enforcement (ICE) and CBP did not have measures for assessing the performance of key immigration enforcement programs. For example, in April 2011 we reported that ICE did not have measures for its overstay enforcement efforts, and in July 2010 that CBP did not have measures for its alien smuggling investigative efforts, making it difficult for these agencies to determine progress made in these areas and evaluate possible improvements. We recommended that ICE and CBP develop performance measures for these two areas. They generally agreed and reported actions underway to develop these measures. In addition, in July 2011, DHS stated that CBP was leading a multiyear effort to develop measures for border security to position the department to be able to assess the impact of security measures, such as tactical infrastructure, on border security. DHS also reported that it has measures for assessing its border security and immigration enforcement efforts, such as measures related to detaining and removing criminal aliens while maintaining compliance with detention standards. However, our work has shown that within key border security and immigration enforcement programs, DHS and its components can strengthen its measures for assessing program results.

In addition, with regard to emergency preparedness and response, we reported that DHS lacks measures for assessing the effectiveness of its preparedness and response efforts. For example, in March 2011 we reported that it has been difficult for the Federal Emergency Management Agency (FEMA) to overcome challenges in its efforts to measure preparedness and establish a system of metrics to assess national preparedness capabilities. In October 2010, we reported that FEMA officials said that evaluation efforts they used to collect data on national preparedness capabilities were useful for their respective purposes, but that the data collected were limited by data reliability and measurement issues related to the lack of standardization in the collection of data. Further, in January 2010 we reported that FEMA faced challenges measuring performance for its Citizen Corps Programs, its partner programs, and the Ready Campaign—community preparedness programs—because it relied on states to verify data for local program

units and was unable to control the distribution of the Ready Campaign messages or measure whether the messages were changing the behavior of individuals.[4] We noted that by examining the feasibility of approaches to verify data on its community preparedness programs, FEMA would be better positioned to begin to explore why programs that no longer exist were disbanded and develop possible strategies for reconstituting local programs or developing new ones. Among other things, we recommended that FEMA examine the feasibility of developing various approaches for ensuring the accuracy of program data.

In July 2011, FEMA reported taking additional action to strengthen its performance measures by, for example, implementing a priority goal focusing on ensuring resilience to disasters by strengthening disaster preparedness and response capabilities, and beginning in fiscal year 2010, requiring its offices to develop and report on activity-level (or operational level) performance measures to align to each of FEMA's budget activity lines. These steps should help FEMA strengthen its performance measurement efforts. However, FEMA should continue to work toward implementing a comprehensive set of measures for assessing national preparedness capabilities.

GAO Contact

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov.

[4] Citizen Corps is coordinated nationally by FEMA and is intended to help coordinate volunteer activities for, among other things, better preparing communities to respond to emergency situations. Citizen Corps programs build on the successful efforts that are in place in many communities around the country to prevent crime and respond to emergencies. Programs that started through local innovation are the foundation for Citizen Corps and this national approach to citizen participation in community safety.

Appendix XV: Risk Management

What This Area Includes

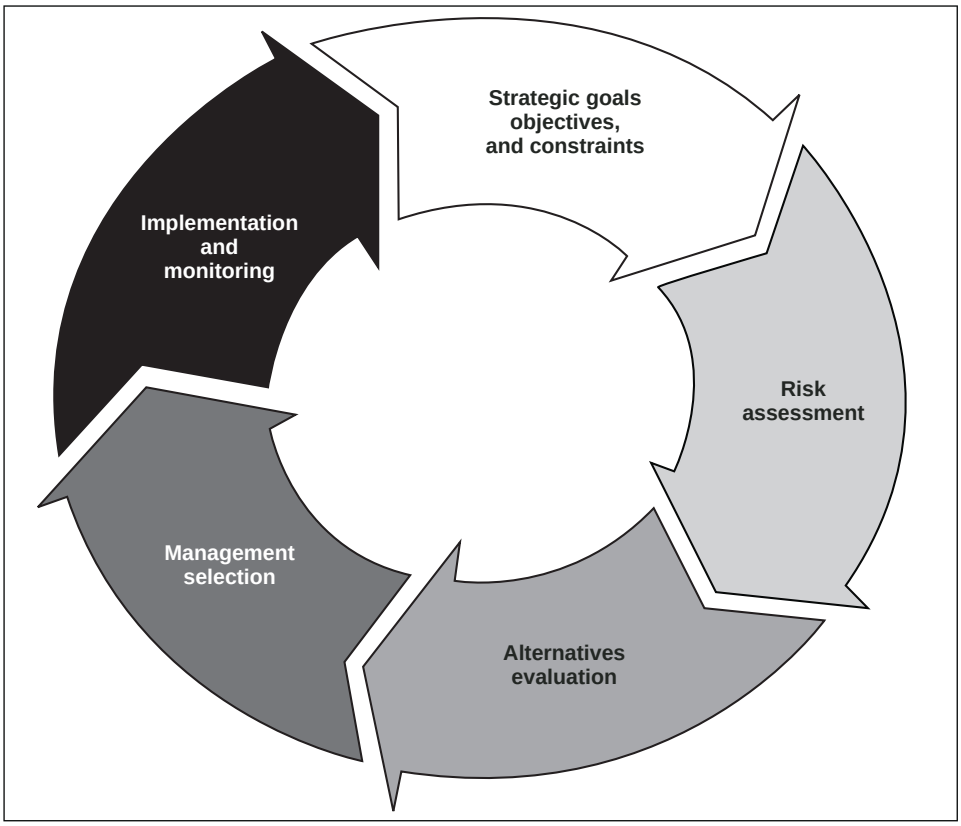
Risk management has been widely supported by the President and Congress as a management approach for homeland security.[1] According to the Department of Homeland Security (DHS), risk information is usually one of many factors—and typically not the sole factor—that departmental decision makers consider when deciding which strategy to pursue. We have previously reported that defining an acceptable, achievable (within constrained budgets) level of risk is imperative to address current and future threats, and on the need to make risk-informed decisions related to homeland security. Many have pointed out, as did the Gilmore and 9/11 Commissions, that the nation will never be completely safe and total security is an unachievable goal.[2] Within its sphere of responsibility, DHS cannot afford to protect everything against all possible threats. As a result, DHS must make choices about how to allocate its scarce resources to most effectively manage risk, and a risk management approach can help inform these decisions.

To provide guidance to agency decision makers, we developed a risk management framework which is intended to be a starting point for applying risk-informed principles. Our risk management framework, shown in figure 2, entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

[1] The *DHS Risk Lexicon* defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. DHS further defines risk as the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence. A threat is defined as natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability is defined as the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Consequence is defined as the effect of an event, incident, or occurrence. DHS, *DHS Risk Lexicon: 2010 Edition* (Washington, D.C.: September 2010).

[2] The Gilmore Commission's full name was the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. The 9/11 Commission was a bipartisan commission chartered to review the circumstances surrounding the September 11, 2001, terrorist attacks, including preparedness for and the immediate response to the attacks, and to provide recommendations designed to guard against future attacks.

Figure 2: GAO Risk Management Framework



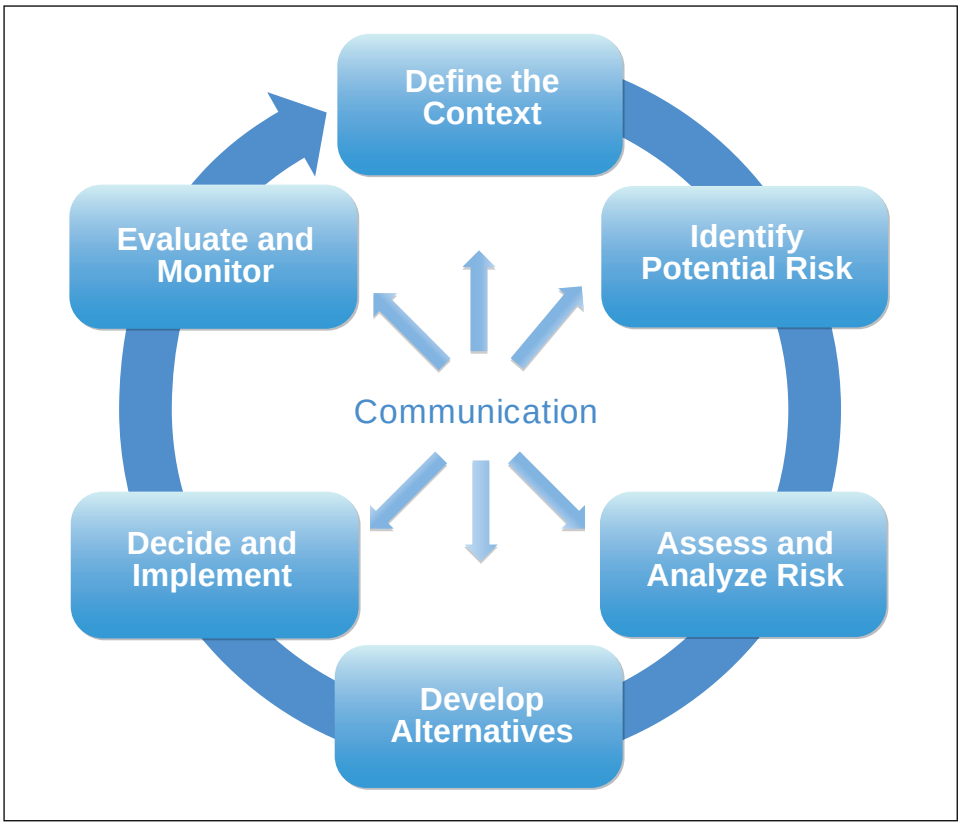
Source: GAO.

The *National Infrastructure Protection Plan*, issued by DHS, includes a risk analysis and management framework for the critical infrastructure community, which generally mirrors our framework. Like our framework, the *National Infrastructure Protection Plan's* risk management framework is a process that continuously uses the results of each step to inform the

activities in both subsequent and previous steps over time.[3] The *National Infrastructure Protection Plan* risk management framework is designed to produce a systematic and comprehensive understanding of risk and ultimately provide for security investments based on this knowledge of risk. In addition, according to DHS, the Secretary's policy for integrated risk management and the department's *Risk Management Fundamentals: Homeland Security Risk Management Doctrine,* identify a risk management process to support decision making at DHS, as shown in figure 3.

[3] In accordance with the Homeland Security Act and in response to Homeland Security Presidential Directive 7, DHS issued, in June 2006, the first *National Infrastructure Protection Plan*, which provides the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. The plan sets forth a risk management framework and details the roles and responsibilities of DHS and other federal, state, regional, local, tribal, territorial, and private sector partners, including how they should use risk management principles to prioritize protection activities within and across sectors.

Figure 3: DHS Risk Management Framework



Source: DHS.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to risk management on which we recently reported, and not areas on which we have not reported or have conducted limited audit work. While this section focuses on key areas on which we have reported, such as risk assessments for transportation modes, DHS has implemented additional efforts related to risk management, such as various risk assessment tools, databases, and coordination mechanisms. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS and its component agencies developed strategies and tools for risk management and conducted risk assessments. However, they should strengthen their use of risk information to inform their

DHS developed and expanded tools for assessing risks within and across its functional areas. However, the department could further strengthen these tools and its use of risk information in making planning and investment decisions.

planning and investment decision-making. DHS took action to develop various strategies, plans, and tools for risk management. For example:

- In 2007 DHS established the Risk Steering Committee, comprised of representatives from DHS's offices and components, to serve as the department's risk management governance body, setting policy and developing guidance for integrating risk management approaches.
- In January 2009 DHS published its *Integrated Risk Management Framework*, which, among other things, calls for DHS to use risk assessments to inform decision-making. Further, in October 2009, under the auspices of the 2010 Quadrennial Homeland Security Review (QHSR), DHS developed the Homeland Security National Risk Assessment methodology for assessing risk across a range of hazards for use by DHS in its decisions on strategy and policy development, planning priorities, resource allocation, and capability requirements development. As part of our ongoing review of DHS's 2010 QHSR, we found that DHS has not yet conducted a national risk assessment, but plans to conduct such an assessment as part of the next QHSR, which DHS plans to initiate in fiscal year 2012.[4]
- In May 2010, the Secretary issued a Policy Statement on Integrated Risk Management, calling for DHS and its partners to manage risks to the nation. DHS reported that it is developing doctrine and guidance to enable DHS to achieve integrated risk management and that DHS's *Integrated Risk Management Framework*, over time, will provide governance, policies, processes, tools, training, and accountability mechanisms for integrated risk management.
- DHS developed the Risk Assessment Process for Informed Decision-making tool to support DHS risk management tradeoffs. According to DHS, this tool has three key deliverables: (1) a quantitative multi-hazard homeland security risk baseline (i.e. annualized expected loss across a range of terrorism, transnational crime, and natural hazard events), (2) a map of major DHS programs to homeland security hazards that shows how programs interact to manage the risk of a specific hazard, and (3) program-based risk reduction analysis that shows the risk reduction of individual programs.
- In June 2010 the Transportation Security Administration (TSA) produced the *Transportation Sector Security Risk Assessment*, which incorporated threat, vulnerability, and consequence to assess risk

[4] We are conducting this work at the request of the Senate Committee on Homeland Security and Governmental Affairs and plan to report on the results later this year.

within and across the various aviation and surface transportation modes, such as freight rail, passenger rail, and pipelines.

In addition, our work shows that DHS and its components conducted risk assessments across a number of areas, but should strengthen these assessments. For example, with regard to surface transportation security, in February 2009 we reported that DHS had conducted threat assessments of the commercial vehicle sector and was in the early stages of conducting vulnerability assessments for this sector. However, we reported that TSA's commercial vehicle threat assessments generally did not identify the likelihood of specific threats, as directed by the *National Infrastructure Protection Plan*, and that TSA had not yet determined the scope, method, and time frame for completing vulnerability assessments. We also noted that TSA had not yet conducted consequence assessments, and as a result, could not be sure that its approach for securing the commercial vehicle sector addressed the highest priority security needs. Moreover, in January 2009 we reported that federal entities, including DHS, had efforts underway to assess threat, vulnerability, and consequence for highway infrastructure, but these efforts were not systematically coordinated among key federal partners and the results were not routinely shared. In August 2010, we further reported that TSA developed a pipeline risk assessment model that combined threat, vulnerability, and consequence to create a risk score for each system. However, we reported that DHS should improve the model's consequence component to take account of additional impacts from a possible pipeline attack, such as public health and safety, as called for in the *National Infrastructure Protection Plan*.

Among other things, we recommended that DHS establish a plan and time frames for conducting commercial vehicle sector risk assessments, to include vulnerability and consequence assessments; establish a mechanism to coordinate risk assessment activities and share results related to highway infrastructure; and develop a plan for improving data in the pipeline risk assessment model to include, for example, more data on the consequence component. TSA generally concurred and took action to address them. For example, in 2010 TSA began conducting vulnerability assessments of significant highway bridges under contract with the U.S. Army Corps of Engineers; submitted to Congress assessments required under the Implementing Recommendations of the 9/11 Commission Act

of 2007, such as those for the trucking and school bus industries;[5] and developed assessments for highway infrastructure, bus, commercial truck, and port interfaces that were incorporated into the *Transportation Sector Security Risk Assessment*. Moreover, in July 2011 TSA reported that it added data columns for consequence and vulnerability components in its pipeline risk ranking tool to address pipelines in highly populated and high consequence areas. These are important actions that should strengthen TSA's risk assessment efforts across the transportation modes. We have not yet assessed these efforts, and thus cannot make an assessment of TSA's efforts.

In addition, with regard to maritime security, the Coast Guard developed a risk assessment model, the Maritime Security Risk Analysis Model, to assess risk across ports. In April 2010, we reported that the Coast Guard had assessed the risks to cruise ships and facilities using this model. However, our work has shown that the Coast Guard has used the model to assess offshore energy facilities, but faces challenges in doing assessments because of difficulties in determining the types of attack scenarios that could cause significant consequences, and in calculating secondary economic effects. In July 2011, the Coast Guard reported that it is working to improve the accuracy, utility, and standardization of its model, as the modeling, simulation, and analysis of terror attack scenarios improves. We are currently conducting work examining the Maritime Security Risk Analysis Model as well as the extent to which DHS is allocating port security resources based on risk.[6] We plan to report the results from this work later this year.

DHS and its components have taken steps to conduct risk assessments, but they have not always incorporated risk information into their planning and investment decision-making. For example, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR) to align DHS's programmatic activities, such as investigating drug smuggling, and its organizational structure to the missions and goals identified in the QHSR.[7] The BUR report identified priority initiatives, such as enhancing

[5] Pub. L. No. 110-53, §§ 1538, 1540(b), 121 Stat. 266, 467, 468 (2007).

[6] We are conducting our work for the Senate committees on Commerce, Science and Transportation Homeland Security and Governmental Affairs, and the House Subcommittee on Border and Maritime Security.

[7] DHS, *Bottom-Up Review Report* (Washington, D.C.: July 2010).

the department's risk management capability, to strengthen DHS's mission performance, improve departmental management, and increase accountability. In our ongoing review of DHS's QHSR, we found that DHS considered various factors in identifying high priority BUR initiatives for implementation in fiscal year 2012, but did not include risk information as one of these factors. Consideration of risk information could help strengthen DHS's prioritization of mechanisms for implementing the QHSR, including determining which BUR initiatives could be implemented in the short or longer term, and the resources required for implementation. We plan to report on the final results of this work later this year.

Also, with regard to transportation security, DHS has not fully utilized risk information in its strategic planning and prioritization efforts. For example, in March 2009 we reported that TSA had developed an approach to prioritization of its security activities based primarily on intelligence instead of comprehensive risk assessments. We reported that DHS had not reviewed or validated the methodology for this approach; thus, TSA lacked assurance that its approach provided the information needed to guide investment decisions to ensure resources were allocated to the highest risks. Further, with regard to planning efforts, in October 2009, we reported that TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based. We noted that lacking such information, DHS could not provide reasonable assurance that its strategy was effectively addressing security gaps, prioritizing investments based on risk, and targeting resources toward security measures that would have the greatest impact. Among other things, we recommended that DHS conduct a complete risk assessment related to TSA's passenger screening program and incorporate the results into the program's strategy. DHS generally concurred and reported actions underway to address them. For example, in July 2011, TSA reported beginning to use a risk management analysis process to analyze the effectiveness and efficiency of potential countermeasures and impact on the commercial aviation system. While these are positive steps, it is too early to assess the extent to which they will improve DHS's use of risk information in strategic planning and investment decision making.

GAO Contact

For additional information about this area, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

Appendix XVI: Information Sharing

What This Area Includes

Since September 11, 2001, terrorist threats and attempted attacks have emphasized the importance of developing a national information sharing capability to efficiently and expeditiously gather, analyze, and disseminate terrorism-related information, such as law enforcement, homeland security, and public safety information. The Department of Homeland Security (DHS) has responsibility for sharing terrorism-related information as appropriate with its state and local partners. In 2005, we designated information sharing for homeland security as high risk because the government faced serious challenges in analyzing information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way to protect against terrorist threats. We have further reported that DHS must effectively share terrorism-related information with state and local law enforcement because they depend on it to maintain awareness of emerging threats and to allocate homeland security resources, among other things. Further, gaps in sharing, such as agencies' failure to link information about the individual who attempted the December 25, 2009, airline bombing, prevented him from being included on the federal government's terrorist watchlist, a tool used by DHS to screen for persons who pose a security risk.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to information sharing on which we have recently reported and not on areas on which we have not reported or conducted limited audit work. Our work has focused primarily on the sharing of terrorism-related information to identify threats and help prevent terrorist incidents. DHS has other ongoing efforts related to information sharing on which we are not reporting, such as information sharing with the government of Canada for emergency management purposes. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS expanded its efforts to share terrorism-related information with its partners, particularly state and local government and private-sector entities. However, DHS could better identify state and local agencies' information needs, set performance measures for assessing results, and streamline its mechanisms for sharing information.

In our February 2011 high-risk update, as well as a July 2011 report, we reported that the government continued to make progress in sharing terrorism-related information among its many security partners, but did not yet have a fully-functioning Information Sharing Environment in place. This environment is an approach intended to facilitate the sharing of terrorism-related information. Specifically, we reported that the Program Manager for the Information Sharing Environment, as well as key security agencies, including DHS, made progress in implementing a discrete set of goals and activities, and are working to establish an "end state vision" that could help better define what the environment is intended to achieve and include. However, these actions have not yet resulted in a fully

functioning environment, and the Program Manager and agencies have not yet identified the incremental costs necessary to implement it or addressed our 2008 recommendation to develop procedures for determining what work remains. DHS is one of the five federal agencies with responsibility for implementing the Environment, and has the lead for sharing information with state, local, tribal, territorial, and private sector partners. Related to this responsibility, DHS has been implementing its information sharing policy and governance structure to improve how it collects, analyzes, and shares homeland security information across the department and with these state and local partners.[1]

DHS expanded and enhanced its sharing of information, but should improve its assistance and services to state and local homeland security partners and streamline some of its information sharing mechanisms. In January 2011, DHS issued a plan for addressing the areas for which it has responsibility under the terrorism-related information sharing high-risk area. DHS identified strategies and initiatives it had planned or underway to address our high-risk criteria and outcomes we identified as important to successfully managing risks that exist due to gaps in information sharing. For example, the plan discussed steps for developing a governance structure for information sharing and beginning efforts to develop a set of metrics for measuring information sharing performance and results. We provided DHS with feedback on this plan. Among other things, we noted the department needs to move toward a system where it accounts for information sharing initiatives against a baseline set of defined capabilities—such as information sharing mechanisms, personnel, and technology—that are needed, to help decision makers weigh progress achieved and remaining to inform investments. Subsequent to our feedback, in July 2011, DHS reported that it had established performance measures for assessing its information sharing efforts. These measures include, for example, the percent of intelligence reports customers rated as “satisfactory” in enabling customers to anticipate emergency threats. DHS plans to report on these metrics beginning in fiscal year 2012. While these are positive steps, our work has shown that developing outcome-based performance measures that gauge information sharing efforts and results would strengthen accountability for these efforts.

[1] DHS has established an Information Sharing Governance Board to identify information sharing priorities, monitor progress in meeting milestones as priorities are identified, and provide assistance as needed.

Specific to its mission to share information with state and local partners, in December 2010 we reported that DHS's Office of Intelligence and Analysis had initiatives underway to identify these partners' information needs and obtain feedback on intelligence products. The office determined information needs—which are owned and controlled by the states—for 9 of the 50 states and was working with the remaining states to identify their needs.[2] However, we reported that the Office of Intelligence and Analysis had not established mutually agreed upon milestones for completing this effort. We also reported that in addition to intelligence products, the office provided a number of other services to its state and local partners—primarily through these partners' fusion centers where homeland security, terrorism, and intelligence information is shared—that had generally been well received by the center officials we contacted. For example, the Office of Intelligence and Analysis deployed more than 60 intelligence officers to fusion centers nationwide to assist state and local partners in areas such as obtaining relevant intelligence products and leveraging DHS capabilities to support their homeland security missions. However, the office had not yet defined how it planned to meet its state and local information-sharing mission by identifying and documenting the specific programs and activities that are most important for executing this mission. Moreover, its performance measures did not allow the office to demonstrate the expected outcomes and effectiveness of programs and activities that support state and local partners.

We recommended that DHS's Office of Intelligence and Analysis establish milestones for identifying the information needs of state and local partners, identify and document priority programs and activities related to its state and local mission, and establish time frames for developing additional related performance measures. DHS concurred and, as of July 2011, reported determining information needs with 26 of 50 states and working to finalize the others. The Office of Intelligence and Analysis also issued a strategic plan in February 2011 that identified goals, objectives, and performance measures for the office's functions. Further, in July 2011, DHS reported that it was developing a guidebook to explain the process that state and major urban area fusion centers should follow to use customer engagement for identifying, documenting, and prioritizing their intelligence questions, information needs, information

[2] In this context, information needs refer to any general or specific subject for which a state or local agency has a continuing need for intelligence.

gaps, and collection requirements. According to DHS, this guidebook will help fusion centers identify and document a more accurate and actionable set of information needs and gaps. These actions should help DHS better assess the performance of its information sharing activities. However, it is too early to assess possible results, since they have only recently been, or are in the process of being, implemented.

Moreover, in September 2010 we reported that since 2001, all 50 states and some major urban areas established fusion centers—totaling 72 centers as of July 2011, according to DHS. These centers have cited DHS grant funding as critical to achieving baseline capabilities—the standards the government and fusion centers have defined as necessary for centers to be considered capable of performing basic functions. To provide data about the baseline capabilities of fusion centers nationwide, DHS and other agencies are conducting an ongoing systematic assessment of fusion centers' capabilities. According to DHS senior officials and fusion center representatives, the results of the assessment are intended to provide centers with the information needed to develop more accurate and specific investment justifications. However, DHS had not set standard performance measures for the centers. We recommended that DHS define the steps it will take to design and implement such a set of measures and commit to a target timeframe for completing them. DHS concurred and stated that it has started to develop a framework to demonstrate the value and impact of the national network of fusion centers, and is using nationwide assessment data to support the development of specific performance measures. These efforts should help DHS strengthen its assessment of fusion centers' performance, but it is too soon to assess results as DHS is in the process of implementing these efforts. As we have reported, if centers are to receive continued federal financial support, it is important that they are also able to demonstrate their impact and value added to the nation's information sharing goals.

Additionally, we have reported that DHS and the Transportation Security Administration (TSA) have taken steps to share surface transportation security information with stakeholders in different sectors. For example, DHS established the Homeland Security Information Network, which was designed to serve as the department's primary information-sharing mechanism for the larger homeland security community engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents under DHS jurisdiction. Within the Homeland Security Information Network, each of the 18 critical infrastructure sectors maintains its own site, and under the transportation

sector, there are sites for different transportation modes, such as public transit. We found in September 2010 that 75 percent of the public transit agencies we surveyed reported being generally satisfied with the security-related information they received.

However, we have identified several challenges to DHS's information sharing efforts for surface transportation security. For example, some public transit agencies cited the need to streamline the information they received, and we identified the potential for overlap between the Public Transportation Information Sharing and Analysis Center,[3] the Public Transit Portal of DHS's Homeland Security Information Network, and the Transportation Security Information Sharing and Analysis Center,[4] which all communicate similar unclassified and security-related information to public transit agencies. Also, preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate that some freight rail stakeholders would prefer to receive more analysis or actionable information from TSA, such as trend analysis of incidents or suggestions for improving security arrangements, that could help predict how certain events may affect rail systems.[5] In addition, DHS and TSA have not developed performance goals and outcome-oriented measures to gauge the effectiveness of their information-sharing networks.

We recommended that DHS establish time frames for a working group of federal and industry officials to assess opportunities to streamline information-sharing mechanisms to reduce any unneeded overlap, and for developing goals and related outcome-oriented performance measures specific to each security information network. DHS concurred, and TSA and industry groups developed a report and associated library, which is intended to streamline the analysis, sharing, and exchange of

[3] The Public Transportation Information Sharing and Analysis Center, which is implemented by the American Public Transportation Association and funded by TSA, collects, analyzes, and distributes security and threat information from the federal government and open sources on a 24/7 basis.

[4] TSA's Office of Intelligence implemented its page on the Homeland Security Information Network in March 2010 as a collaborative information-sharing platform for all transportation modes, including public transit.

[5] This work is being conducted in response to a mandate in the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007). We plan to issue our findings on this work later this year.

intelligence and security information that had been disseminated by multiple sources. Further, in July 2011 TSA reported that it and key industry groups were engaged in an ongoing process to develop, improve, and refine its information sharing mechanisms. In addition, TSA reported that it continues to work with its stakeholders to determine how available intelligence and other security incident data can be leveraged to provide stakeholders with meaningful information to help guide actions in the field. We are continuing to assess TSA's efforts related to sharing security information with stakeholders in the aviation, rail, and highway modes and will report the final results later this year.

GAO Contact

For additional information about this area, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov.

Appendix XVII: Partnerships and Coordination

What This Area Includes

The Department of Homeland Security (DHS) provides federal leadership for homeland security, but also plays a large role in coordinating the homeland security activities of other federal, state, local, private sector, and international stakeholders. We reported that successful partnering and coordination involves collaborating and consulting with stakeholders to develop and agree on goals, strategies, and roles to achieve a common purpose; identify resource needs; establish a means to operate across agency boundaries, such as compatible procedures, measures, data, and systems; and agree upon and document mechanisms to monitor, evaluate, and report to the public on the results of joint efforts. If these entities do not effectively coordinate their implementation activities, they may waste resources by creating ineffective and incompatible pieces of a larger security program. For example, because the private sector owns or operates a majority of the nation's critical infrastructure, DHS must partner with individual companies and sector organizations to protect vital national infrastructure, such as the nation's water supply, transportation systems, and chemical facilities.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to partnerships and coordination on which we have recently reported. We are generally not addressing areas on which we have not reported or have conducted limited audit work. For example, DHS has ongoing efforts related to coordinating with homeland security partners within and across its various mission areas and programs, such as for combating nuclear terrorism and conducting biological research to support the nation's biodefense preparedness. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS made progress in coordinating its programs and activities with homeland security partners, but could strengthen its efforts to better ensure that partners' information needs are met and provide enhanced oversight of coordination mechanisms.

DHS made progress in coordinating its programs and activities with homeland security partners, but should strengthen its coordination by, among other things, better meeting the information needs of private sector partners and providing oversight of coordination mechanisms. DHS has strengthened its coordination with homeland security partners in a number of functional areas, such as aviation security, critical infrastructure protection, border security, and emergency preparedness and response, but should further enhance coordination efforts. For example, with regard to aviation security, in December 2010, we reported that DHS and the Transportation Security Administration (TSA) worked on coordinating security standards and practices to enhance security with foreign partners—a process known as harmonization. DHS and TSA did so through increased global outreach,

coordination of standards and practices, use of enhanced technology, and assessments of foreign airports. We also reported that DHS and TSA coordinated with foreign governments to harmonize air cargo security practices to address the statutory mandate to screen 100 percent of air cargo transported on U.S.-bound passenger aircraft.[1] In July 2011, TSA reported that it had requested air carrier feedback on their ability to accomplish 100 percent of screening on international inbound air cargo by December 2011, and is evaluating industry comments to finalize its strategy and establish a feasible timeline for implementing the screening requirement.

With regard to critical infrastructure protection, in September 2010 we reported that DHS's National Protection and Programs Directorate (NPPD) operates the Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists, called Protective Security Advisors, to local communities throughout the country. These advisors lead NPPD's efforts in these locations and act as a link between state, local, tribal, and territorial organizations and DHS infrastructure mission partners. DHS also reported that these advisors work to maintain relationships with the private sector and local communities to help foster effective information sharing and disseminate information to the private sector during times of increased threat.

Further, in July 2010 we reported on the expectations of public and private sector stakeholders for their cyber-related public-private partnerships. The expectations that the partners identified included timely and actionable cyber-threat information and alerts and a single centralized government cybersecurity organization to coordinate government efforts. Federal partners, including DHS, took steps to help address the expectations of the private sector, including developing new information-sharing arrangements and expanding the number of private sector individuals with security clearances. However, much work remains in ensuring that the expectations of public and private stakeholders are fully met. For example, less than one-third of private sector respondents reported that they were receiving actionable cyber threat information and alerts from federal partners to a great or moderate extent. We recommended that DHS work with its federal and private sector partners to enhance information-sharing efforts. DHS concurred and reported in

[1] See 49 U.S.C. § 44901(g).

July 2011 that it was taking additional action by, for example, establishing cybersecurity working groups, interagency coordination groups, and a performance measure for fiscal year 2012 to seek public and private sector feedback on the extent to which DHS cybersecurity products are actionable and timely. However, as DHS is in the processing of implementing these efforts, it is too early to assess their effectiveness.

With regard to border security, in December 2010 we reported that federal, state, local, tribal, and Canadian law enforcement partners reported improved DHS coordination to secure the northern border. For example, interagency forums helped establish a common understanding of border security threats, while joint operations helped to achieve an integrated and effective law enforcement response. However, challenges remained in sharing information and resources useful for operations along the northern border. For example, partners in all four sectors we visited cited ongoing challenges in sharing information and resources for daily border security-related to operations and investigations, and we reported that oversight by management at the component and local level had not ensured consistent compliance with provisions of interagency agreements, such as those related to information sharing.[2] In November 2010, we reported that information sharing and communication among the Departments of Agriculture, Homeland Security, and Interior for securing federal and tribal lands along the border had increased, but that critical gaps remained. For example, these agencies had established forums and liaisons to exchange information; however, in one sector they did not coordinate to ensure that federal land law enforcement officials maintained access to threat information and compatible secure radio communications for daily operations. Coordination in these areas could better ensure officer safety and an efficient law enforcement response to illegal activity.

Moreover, we reported in February 2008 that the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program office, which is to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information, had not fully defined its relationships with other immigration

[2] We visited the Blaine, Spokane, Detroit, and Swanton sectors. While we could not generalize our work from these visits to all locations along the northern border, the information we obtained provided examples of the way in which DHS and other federal agencies coordinated their efforts with northern border partners.

and border management programs or its approaches relative to addressing outcomes shared by those programs. As a result, we concluded that the department risked suboptimizing how its programs collectively supported its immigration and border management goals and objectives. We have made recommendations to DHS to strengthen its border security coordination efforts. For example, we recommended that DHS provide oversight to ensure efficient use of border security interagency forums and compliance with interagency agreements; take necessary action to ensure that personnel conduct early and continued consultations to coordinate on, among other things, threat information for federal lands that is timely and actionable; and fully define relationships between the US-VISIT program and other programs.

DHS concurred and reported, for example, that it plans to review the inventory of interagency forums through its strategic and operational planning efforts to assess efficiency and identify challenges. Further, in July 2011, the US-VISIT program office reported taking action to coordinate with other immigration and border security programs. For example, it reported that it had established a governance board to enhance border security solutions to meet congressional mandates, and supported the expansion of immigration enforcement related programs, such as Secure Communities through which U.S. Immigration and Customs Enforcement works with state and local law enforcement agencies to identify and remove immigration violators. While these are positive steps, DHS needs to demonstrate that these efforts have helped the department to fully define relationships between the US-VISIT program and other programs.

In addition, with regard to emergency preparedness and response and chemical, biological, radiological, and nuclear incident preparedness, in June 2011 we reported that DHS and the Department of Health and Human Services coordinated with each other and with other federal departments to develop chemical, biological, radiological, and nuclear risk assessments, but neither department had written procedures for developing these assessments. Our best practices for interagency collaboration and federal standards for internal control indicate that agencies can best enhance and sustain coordination by adopting key practices, such as defining desired common outcomes, agreeing on roles and responsibilities, and developing written policies and procedures to help ensure that management directives are enforced. We reported that such practices and standards should help DHS and the Department of Health and Human Services institutionalize their agreements on these sensitive and technical issues to better ensure coordination, collaboration,

and continuity beyond the tenure of any given official or individual office, and recommended that the departments develop these practices. DHS concurred with our recommendation.

GAO Contact

For additional information about this area, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

Appendix XVIII: Developing and Deploying New Technologies for Homeland Security

What This Area Includes

Since beginning operations in 2003, the Department of Homeland Security (DHS) has spent billions of dollars on research and development of technologies and other countermeasures to address threats and conduct its missions. DHS programs represent hundreds of billions of dollars in life-cycle costs and support a wide range of missions and investments, including border surveillance and screening equipment, nuclear detection equipment, information systems that help detect and interdict the planning of terrorist acts, and technologies used to screen airline passengers and baggage for explosives. Within DHS, the Science and Technology Directorate (S&T) has the authority to coordinate overall research and development efforts to improve homeland security. Among other things, S&T works with DHS components to provide assistance in researching and developing technologies to meet their specific missions, while the components themselves are responsible for developing, testing, and acquiring these technologies. For instance, the Transportation Security Administration (TSA) works with S&T to research, develop, and deploy technologies to, for example, screen airline passengers and their baggage. DHS's Domestic Nuclear Detection Office (DNDO) is responsible for developing, acquiring, and supporting the deployment of programs and systems to detect and report on attempts to develop, transport, or use unauthorized nuclear explosive, fissile, or radiological materials or explosives in the United States.

For the purposes of this report, we are generally highlighting examples of DHS efforts related to developing and deploying new technologies on which we have recently reported, and are generally not addressing areas on which we have not reported or have conducted limited audit work. While this section addresses examples on which we have reported, which focus on DHS's efforts related to technologies for border, transportation, and maritime security, DHS has other efforts related to developing and deploying new technologies, such as technologies for intelligence. DHS also reported that it has taken steps intended to formalize requirements definition and technology development. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS took action to develop and deploy new technologies to help implement its homeland security missions. However, the department experienced challenges in managing its efforts to develop and deploy new technologies, including implementing technologies that did not meet intended requirements and were not appropriately tested and evaluated, and has not consistently completed analyses of costs and benefits before technologies were implemented.

DHS took action to develop and deploy new technologies to help meet its homeland security missions. However, in some instances DHS pursued acquisitions without ensuring that the technologies met defined requirements and faced challenges in conducting and documenting testing and evaluation and performing cost-benefit analyses. DHS developed and deployed various technologies within its functional areas, including maritime and transportation security. For example, in September 2010, we reported that DHS made progress in researching and developing container security technologies. Specifically, we reported that since fiscal year 2004 DHS conducted research and development for four container security technology projects to monitor cargo tampering and, according to DHS, provide a global communication system to securely transmit information to DHS components responsible for port security. Moreover, in June 2010 we reported that DHS made significant progress in deploying radiation detection equipment to scan cargo and conveyances entering the United States through fixed land and sea ports of entry for nuclear and radiological materials. Specifically, we reported that DHS deployed more than 1,400 radiation portal monitors to ports of entry. Further, TSA continues to deploy technologies to screen checked baggage. As of July 2011, TSA reported that it had about 2,300 explosives detection systems in its fleet, about 1,900 of which were deployed at airports in the United States.[1] At airports and terminals that do not use these systems, explosives trace detection machines are used for primary checked-baggage screening, typically at smaller airports.[2] As of July 2011, TSA estimated that there were about 5,000 explosives trace detection machines used for the primary or secondary screening of checked baggage at U.S. commercial airports. In addition, in June 2010 we reported that DHS, the United States Postal Service, and the Department of Defense developed and implemented technologies to sample the air and test for specific biological agents. In particular, DHS's BioWatch program had been implemented in more than 30 metropolitan areas and tests for the presence of multiple biological agents.

[1] An explosives detection system uses computed tomography technology to automatically measure the physical characteristics of objects in baggage. The system automatically triggers an alarm when objects that exhibit the physical characteristics of explosives are detected.

[2] An explosives trace detection machine is used to chemically analyze trace materials after a human operator swabs checked baggage to identify any traces of explosive material.

However, our work has shown that DHS made acquisition decisions without ensuring that the systems met program and performance requirements.

- In September 2010, we reported that DNDO was simultaneously engaged in the research and development phase while planning for the acquisition phase of its cargo advanced automated radiography system to detect certain nuclear materials in vehicles and containers at ports. DNDO pursued the acquisition and deployment of the cargo advanced automated radiography system without fully understanding that it would not fit within existing inspection lanes at ports of entry. This occurred because, during the first year or more of the program, DNDO and U.S. Customs and Border Protection (CBP) had few discussions about operating requirements for primary inspection lanes at ports of entry. DHS announced the termination of the program in 2010.
- In July 2011, we reported that TSA revised its explosives detection system requirements to better address current threats in screening checked baggage, and plans to implement these requirements in a phased approach. However, we reported that some number of systems in TSA's fleet was configured to detect explosives at the levels established in the 2005 requirements and that the remaining systems were configured to detect explosives at 1998 levels. When TSA established the 2005 requirements, it did not have a plan with time frames to deploy the explosives detection systems to meet the new requirements. We recommended that TSA develop a plan to deploy and operate explosives detection systems to meet the most recent requirements. TSA concurred and, in July 2011, reported that it intends to finalize a plan by the fourth quarter of fiscal year 2012.

DHS also encountered challenges in conducting and documenting testing and evaluation of its technologies. Our prior work identified that the failure to resolve problems discovered during testing can sometimes lead to costly redesign and rework at a later date, and that addressing such problems during the testing and evaluation phase before acquiring systems can help agencies avoid future cost overruns. For example:

- In June 2011 we reported that S&T's Test & Evaluation and Standards Office, responsible for overseeing test and evaluation of DHS's major acquisition programs, reviewed or approved test and evaluation documents and plans for programs undergoing testing, and conducted independent assessments for the programs that completed operational testing. DHS senior level officials considered the office's assessments and input in deciding whether programs were ready to

proceed to the next acquisition phase. However, the office did not consistently document its review and approval of components' test agents—a government entity or independent contractor carrying out independent operational testing for a major acquisition. In addition, the office did not document its review of other component acquisition documents, such as those establishing programs' operational requirements.

- In March 2011, we reported that the independent testing and evaluation of the Secure Border Initiative Network's virtual fence Block 1 capability to determine its operational effectiveness and suitability was not complete at the time DHS reached its decision regarding the future of the Secure Border Initiative Network, or requested fiscal year 2012 funding to deploy the new Alternative (Southwest) Border Technology.[3] We reported that because the new Alternative (Southwest) Border Technology incorporates a mix of technology that includes an Integrated Fixed Tower surveillance system similar to that currently used in the Secure Border Initiative Network, such testing and evaluation could have informed DHS's decision about moving forward with the new technology deployment.
- In September 2010, we reported that S&T's master plans for conducting operational testing of container security technologies did not reflect all of the operational scenarios that CBP was considering for implementation. For example, S&T did not include certain scenarios necessary to test how a cargo container would be transported throughout the maritime supply chain. Until the container security technologies are tested and evaluated consistent with all of the operational scenarios, S&T cannot provide reasonable assurance that the technologies will function as intended.

We recommended, among other things, that S&T develop mechanisms to document its review of component acquisition documentation, and that DHS test and evaluate the container security technologies consistent with all of the operational scenarios DHS identified for potential implementation. DHS concurred and reported actions underway to address them, such as drafting a memorandum on the document review

[3] Secure Border Initiative Network Block 1 is a surveillance, command, control, communications, and intelligence system fielded in parts of Arizona that is intended to mitigate or eliminate vulnerabilities along the international border between ports of entry. Block 1 is an element of DHS's Secure Border Initiative, a comprehensive, multiyear plan to secure the borders of the United States and reduce illegal cross border activities such as smuggling of economic migrants, illegal drugs, and people with terrorist intent.

process. Further, in July 2011, S&T and CBP reported starting a joint pilot program to implement a new supply chain security technology on selected rail and truck cargo routes from Mexico and Canada into the United States to evaluate land cargo security devices intended to monitor unauthorized door openings or anomalies and to provide encrypted in-transit tracking.

In addition, DHS has not consistently included cost-benefit analyses in its acquisition decision making. Our prior work shows that cost-benefit analyses help decision makers assess and prioritize resource investments and consider potentially more cost-effective alternatives. 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.[4] 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 DNDO'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. At that time, DNDO officials stated that they planned to update the cost-benefit analysis. In July 2011, DHS announced that DNDO and CBP would end the advanced spectroscopic portal project as originally conceived given the challenges the program faced. DHS reported that it plans to deploy the existing units to field locations to gather operational data to support future planning efforts.

In June 2011, DHS reported that it is strengthening its investment and acquisition management processes across the department by implementing a decision-making process at critical phases throughout the investment life cycle. For example, DHS reported that it plans to establish a new model for managing departmentwide investments across their life cycles. Under this plan, S&T would be involved in each phase of the

[4] We later estimated these costs to be over $2 billion.

investment life cycle and participate in new councils and boards DHS is planning to create to help ensure that test and evaluation methods are appropriately considered as part of DHS's overall research and development investment strategies. In addition, DHS reported that the new councils and boards it is planning to establish would be responsible for, among other things, making decisions on research and development initiatives based on factors such as viability and affordability, and overseeing key acquisition decisions for major programs using baseline and actual data. According to DHS, S&T will help ensure that new technologies are properly scoped, developed, and tested before being implemented. In July 2011, S&T reported that it established a new group to work with DHS components to, among other things, help ensure that operational requirements are completely specified and validated and that comprehensive cost-benefit analyses are performed to identify the best alternative for meeting identified mission needs. However, as DHS has recently established this group, it is too soon to assess its effectiveness. DHS also reports that it is working with components to improve the quality and accuracy of cost estimates and increased its staff during fiscal year 2011 to develop independent cost estimates, a best practice, to ensure the accuracy and credibility of program costs. DHS reports that four cost estimates for level 1 programs have been validated to date.[5] The actions DHS reported taking or underway to address the management of its acquisitions and the development of new technologies are positive steps and, if implemented effectively, could help the department address a number of these challenges.

GAO Contact

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov.

[5] Levels are determined by the life-cycle cost of the program, not the procurement cost. Level 1 (major acquisition) life-cycle cost is identified at or above $1 billion dollars.

Appendix XIX: Comments from the Department of Homeland Security

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

Homeland Security

August 31, 2011

Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-11-881, "DEPARTMENT OF HOMELAND SECURITY: Progress Made and Work Remaining in Implementing Homeland Security Missions Ten Years after 9/11"

Dear Ms. Berrick:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report. The Department concurs with GAO's conclusion that "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 …". As described in the DHS progress report on fulfilling 9/11 Commission recommendations[1], released by Secretary of Homeland Security Janet Napolitano in July 2011, America is a stronger, safer and more resilient country because of the work DHS and its many partners do every day.

A Changed Security Environment

Following the terrorist attacks of September 11, 2001, Congress moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, local, tribal, and territorial capabilities to prepare for, respond to, and recover from threats and disasters at home. A key element of Congress's vision for a new security framework included the creation of DHS in March 2003, bringing together 22 separate agencies and offices into a single, Cabinet-level department.

[1] DHS. *Implementing 9/11 Commission Recommendations: Progress Report 2011.* http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf

1

Since its inception, DHS has made significant progress in securing the nation from terrorism. Comparing today's security architecture to what existed in 2001 illustrates how far we have come in making the country safer and more secure today than it was a decade ago. The following examples highlight a few of the Department's many accomplishments:

Visa Security: Since 2001, DHS has created and managed the Visa Security Program, which is now operational at 19 posts in 15 countries. Through this program, Immigration and Customs Enforcement deploys trained special agents overseas to high-risk visa activity posts to conduct targeted, in-depth reviews of particular visa applications and applicants before they reach the United States.

Border Security: Since 2001, the Department has deployed unprecedented levels of personnel, technology, and resources to the Nation's borders. DHS has increased the number of civilian boots on the ground from approximately 9,800 Border Patrol agents in 2001 to more than 20,800 today.

Fusion Centers: Since 2001, 72 fusion centers have been created to serve as focal points for the receipt, analysis, gathering, and sharing of threat and vulnerability-related information. DHS has provided personnel, grant funding, technical assistance, security clearances, and access to classified networks to help fusion centers achieve and maintain critical operational capabilities. These fusion centers allow the Intelligence Community to identify the common threads that can tie a seemingly minor crime to the larger threat picture, an essential capability that was not in existence just ten years ago.

Passenger Screening and Prescreening: Since 2001, DHS has developed the capacity to prescreen 100 percent of the 14 million passengers flying weekly to, from, and within the U.S. against government watch lists, enabling the Department to identify individuals who are on the "No Fly" list and recommend others for additional screening. Ten years ago, screening of passengers coming to the United States was limited to the visa process and inspection of a person by an immigration officer at the port of entry. Additionally, the Transportation Security Administration (TSA) has deployed roughly 50,000 Transportation Security Officers at more than 450 airports nationwide. TSA has also accelerated the deployment of new technologies to detect the next generation of threats.

In-flight Security: Since 2001, Federal Air Marshals have greatly increased in number, from 33 to thousands in 2011, and are now deployed across the aviation system based on risk. The Federal Flight Deck Officer program allows qualified pilots to use firearms to defend the cockpit and TSA runs a crewmember behavior recognition and response training program. Additionally, the hardening of cockpit doors prevents unauthorized access to the flight deck. Over the past ten years, these efforts have significantly enhanced the safety and security of passengers on board.

Surface Transportation Security: Since 2001, DHS has strengthened efforts in the surface domain to reduce security vulnerabilities and to strengthen resilience against terrorist attacks. For example, DHS has deployed 25 Visible Intermodal Prevention and Response (VIPR) Teams to protect surface transportation, provide deterrent and

2

detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities.

International Information Sharing: Since 2001, eighteen countries have joined the United States to share information about terrorists and criminals to prevent them from traveling freely between countries.

Chemical, Biological, Radiological, and Nuclear (CBRN) Threats: Since 2001, DHS has made significant progress in assessing risks posed by CBRN threats and developing and deploying capabilities to detect and mitigate those threats. From BioWatch to an interagency-approved Global Nuclear Detection Architecture Strategic Plan, the Department is systemically addressing the needs of the Nation to reduce the threat of CBRN terrorism. The Department appreciates GAO's acknowledgement that "DHS made progress in assessing risks posed by CBRN threats."

Emergency Communications: Since 2001, FEMA has continued to support state, local, tribal, and territorial partners' efforts to enhance their emergency communications capabilities through grants and technical assistance. Additionally, in July 2008, DHS issued the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide.

Not only has the Department made significant progress in securing the Nation from terrorism, it also has achieved measurable success developing a Nation that is resilient to natural disasters and threats of all kind. The Department appreciates GAO's acknowledgement that DHS "expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; supported state, local, and tribal partners' disaster response capabilities; and enhanced emergency communications."

A Strategic View of Homeland Security

In February 2010, DHS issued its first Quadrennial Homeland Security Review (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, tribal, and territorial government agencies; the private sector; and nongovernmental organizations.[2] 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. The report also identifies goals and objectives for maturing and strengthening the homeland security enterprise.

This first QHSR report has set the stage for detailed analyses of homeland security capabilities and requirements. This report will drive Department progress by redefining the homeland security missions and setting prioritized goals, objectives, and strategic outcome statements for each mission, and guiding all homeland security stakeholders toward common

[2] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010).

3

goals and objectives. A coordinated approach that promotes unity of effort will provide the foundation to combat current, emerging, and future threats to the homeland.

The Department appreciates GAO's willingness to align its report to the five new homeland security missions identified in the QHSR.

Report's Limited Scope

DHS acknowledges GAO's work documenting the progress the Department has made in enhancing the nation's security and the challenges that still exist. However, as GAO states, the report "does not address . . .all of DHS's homeland security-related activities and efforts." Additionally, as GAO notes, its assessments of the progress in each area is not comprehensive because GAO and the DHS Office of Inspector General (OIG) have completed varying degrees of work for each of the ten functional areas discussed in the report.

In fact, there are a number of DHS activities not reflected in the GAO report that demonstrate progress the Department has made in preparing the nation for threats. For example, the report does not acknowledge certain DHS programs, such as the Western Hemisphere Travel Initiative (WHTI), which have improved security to the United States. WHTI imposes secure identity and citizenship documentation requirements, and its implementation has significantly expedited legitimate travel through improved Port of Entry processing. The report also does not mention some of the improvements resulting from the Department's increased coordination across the Federal government, as exemplified by the analysis of travel-related data. While watch lists existed prior to 9/11, they were neither coordinated nor consolidated to the degree and depth that they are now. Today, four centers across the Federal government provide information regarding potential terrorist travel: the Federal Bureau of Investigation's Terrorist Screening Center, National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center. For additional information on other key areas of progress, see the Department's recently released report that highlights progress fulfilling specific 9/11 Commission recommendations.[3]

Continuing Work with GAO

DHS senior leadership, including the Secretary and Deputy Secretary, have demonstrated a strong and continuing commitment to building and strengthening the Department's relationship with GAO in a mutually beneficial and productive manner. DHS has worked vigorously to close out recommendations from the GAO and OIG, and has made notable progress. In fact, DHS recently developed a strategic framework to manage risk and detailed corrective action plans to address each one of GAO's high risk recommendations. Last year, Secretary Napolitano also signed a Management Directive on relations between DHS and GAO concerning statutorily authorized GAO reviews of DHS activities. The new Directive played an essential role during this engagement as subject matter experts from across the Department worked to provide updated information and documentation to their GAO counterparts. The Department appreciates GAO's receptiveness to our input, and looks forward to continuing our dialogue to further enhance GAO's understanding of all DHS has done and is currently doing to make America a stronger, safer and more resilient nation.

[3] DHS. *Implementing 9/11 Commission Recommendations: Progress Report 2011.* http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf

4

Again, thank you for the opportunity to review and comment on this draft report. I look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

5

Appendix XX: GAO Contact and Staff Acknowledgments

GAO Contact

Cathleen A. Berrick (202) 512-3404 or berrickc@gao.gov

Staff Acknowledgments

In addition to the person named above, Rebecca Gambler, Assistant Director; Taylor Matheson, Analyst-in-Charge; Melissa Bogar; Susan Czachor; Lorraine Ettaro; Sarah Kaczmarek; Tracey King; Dawn Locke; Jan Montgomery; Jessica Orr; and Meghan Squires made key contributions to this report. Other contributors to this report included Joel Aldape; David Alexander; Gene Aloise; Rodell Anderson; Aditi Archer; Sarah Arnett; Neil Asaba; Ben Atwater; Jonathan Bachman; Charles Bausell; Claudia Becker; Scott Behen; Carolyn Blocker; David Bruno; Carissa Bryant; Rochelle Burns; Alicia Cackley; Stephen Caldwell; Lisa Canini; Caitlin Carlberg; Tammy Conquest; Christopher Currie; Ryan Consaul; Frances Cook; Joseph Cruz; Anthony DeFrank; Davi D'Agostino; Kay Daly; Deborah Davis; Katherine Davis; Vanessa Dillard; Michael Dino; Rick Eiserman; Eric Erdman; Jeanette Espinola; Alana Finley; Edward George; Robin Ghertner; Michael Gilmore; Kathryn Godfrey; Robert Goldenkoff; Mark Goldstein; Barbara Guffy; Geoffrey Hamilton; Christopher Hatscher; Brent Helt; David Hinchman; Richard Hung; John Hutton; William O. Jenkins, Jr.; Amanda Jones; Yvonne Jones; Valerie Kasindi; Christopher Keisling; Anjalique Lawrence; Michael Lenington; Eileen Larence; Marya Link; Thomas Lombardi; Stephen Lord; Robert Lowthian; Jessica Lucas Judy; David Lysy; Gary Malavenda; Kush Malhotra; David Maurer; Linda Miller; Lara Miklozek; Anthony Moran; Steve Morris; John Mortin; Gary Mountjoy; Suzanne Murphy; Robin Nye; Jean Orland; Sabine Paul; David Powner; Paula Rascona; Janay Sam; Debra Sebastian; Richard M. Stana; Kevin Tarmann; Nathan Tranquilli; Katherine Trimble; Meg Ullengren; Sarah Veale; Gregory Wilshusen; Michelle Woods; and Edwin Woodward.

Related Reports

Aviation Security

GAO. *Aviation Security: TSA Has Taken Actions to Improve Security, but Additional Efforts Remain.* GAO-11-807T. Washington, D.C.: July 13, 2011.

GAO. *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed.* GAO-11-740. Washington, D.C.: July 11, 2011.

GAO. *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives.* GAO-11-657. Washington, D.C.: May 10, 2011.

GAO. *Aviation Security: Progress Made, but Challenges Persist in Meeting the Screening Mandate for Air Cargo*. GAO-11-413T. Washington, D.C.: March 9, 2011.

GAO. *Aviation Security: TSA's Revised Cost Comparison Provides a More Reasonable Basis for Comparing the Costs of Private-Sector and TSA Screeners*. GAO-11-375R. Washington, D.C.: March 4, 2011.

GAO. *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*. GAO-11-318SP. Washington, D.C.: March 1, 2011.

GAO. *Aviation Security: TSA Has Made Progress but Faces Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft*. GAO-10-446. Washington, D.C.: June 28, 2010.

GAO. *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*. GAO-10-763. Washington, D.C.: May 20, 2010.

GAO. *GAO Review of the Department of Homeland Security's Certification of the Secure Flight Program—Cost and Schedule Estimates.* GAO-10-535R. Washington, D.C.: April 5, 2010.

GAO. *Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain*. GAO-10-484T. Washington, D.C.: March 17, 2010.

GAO. *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers.* GAO-10-43. Washington, D.C.: November 18, 2009.

GAO. *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*. GAO-10-128. Washington, D.C.: October 7, 2009.

GAO. *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls.* GAO-09-399. Washington, D.C.: September 30, 2009.

GAO. *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation.* GAO-09-492. Washington, D.C.: March 27, 2009.

GAO. *Aviation Security: Federal Air Marshal Service Has Taken Actions to Fulfill Its Core Mission and Address Workforce Issues, but Additional Actions Are Needed to Improve Workforce Survey*. GAO-09-273. Washington, D.C.: January 14, 2009.

GAO. *Aviation Security: TSA's Cost and Performance Study of Private-Sector Airport Screening*. GAO-09-27R. Washington, D.C.: January 9, 2009.

GAO. *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*. GAO-08-1024T. Washington, D.C.: July 24, 2008.

GAO. *Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Continue to Progress, but More Work Remains.* GAO-08-651T. Washington, D.C.: April 15, 2008.

GAO. *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*. GAO-08-456T. Washington, D.C.: February 28, 2008.

GAO. *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and*

Documentation of Proposed Changes Could Be Improved. GAO-07-634. Washington, D.C.: April 16, 2007.

GAO. *Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems*. GAO-05-365. Washington, D.C.: March 15, 2005.

Department of Homeland Security Office of Inspector General. *Transportation Security Administration's Management of Its Screening Workforce Training Program Can Be Improved,* OIG-11-05. Washington, D.C.: October 26, 2010.

Department of Homeland Security Office of Inspector General. *Transportation Security Administration's Controls over SIDA Badges, Uniforms, and Identification Cards*, OIG-08-92. Washington, D.C.: September 12, 2008.

Chemical, Biological, Radiological, and Nuclear Threats

GAO. *Combating Nuclear Smuggling: DHS has Developed a Strategic Plan for its Global Nuclear Detection Architecture, but Gaps Remain.* GAO-11-869T. Washington, D.C.: July 26, 2011.

GAO. *National Preparedness: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments.* GAO-11-606. Washington, D.C.: June 21, 2011.

GAO. *DHS Science and Technology: Additional Steps Needed to Ensure Test and Evaluation Requirements are Met.* GAO-11-596. Washington, D.C.: June 15, 2011.

GAO. *Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps*. GAO-10-883T. Washington, D.C.: June 30, 2010.

GAO. *Biosurveillance: Efforts to Develop a National Biosurveillance Capability Need a National Strategy and a Designated Leader*. GAO-10-645. Washington, D.C.: June 30, 2010.

GAO. *Biosurveillance: Developing a Collaboration Strategy Is Essential to Fostering Interagency Data and Resource Sharing*. GAO-10-171. Washington, D.C.: December 18, 2009.

GAO. *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology,* GAO-09-655. Washington, D.C.: May 21, 2009.

GAO. *Nuclear Detection: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities*. GAO-09-257. Washington, D.C.: January 29, 2009.

GAO. *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors.* GAO-09-804T. Washington, D.C.: June 25, 2009.

GAO, *Combating Nuclear Smuggling: DHS's Phase 3 Test Report on Advanced Portal Monitors Does Not Fully Disclose the Limitations of the Test Results*, GAO-09-979. Washington, D.C.: September 30, 2008.

Critical Infrastructure Protection—Physical Assets

GAO. *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*. GAO-11-688T. Washington, D.C.: June 14, 2011.

GAO. *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*. GAO-10-772. Washington, D.C.: September 23, 2010.

GAO. *Homeland Security: Preliminary Observations on the Federal Protective Service's Workforce Analysis and Planning Efforts*. GAO-10-802R. Washington, D.C.: June 14, 2010.

GAO. *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*. GAO-10-296. Washington, D.C.: March 5, 2010.

GAO. *Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts*. GAO-09-604. Washington, D.C.: June 26, 2009.

GAO. *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*. GAO-09-243. Washington, D.C.: April 21, 2009.

GAO. *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*. GAO-09-492. Washington, D.C.: March 27, 2009.

GAO. *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*. GAO-09-57. Washington, D.C.: January 30, 2009.

Department of Homeland Security Office of Inspector General, *Efforts to Identify Critical Infrastructure Assets and Systems,* OIG-09-86. Washington, D.C.: June 30, 2009.

Surface Transportation Security

GAO. *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*. GAO-11-688T. Washington, D.C.: June 14, 2011.

GAO. *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach.* GAO-10-895. Washington, D.C.: September 22, 2010.

GAO. *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes.* GAO-10-867. Washington, D.C.: August 4, 2010.

GAO. *Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Efforts.* GAO-10-650T. Washington, D.C.: April 21, 2010.

GAO. *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*. GAO-09-678. Washington, D.C.: June 24, 2009.

GAO. *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*. GAO-09-491. Washington, D.C.: June 8, 2009.

GAO. *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored.* GAO-09-243. Washington, D.C.: April 21, 2009.

GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation.* GAO-09-492. Washington, D.C.: March 2009.

GAO. *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector.* GAO-09-85. Washington, D.C.: February 27, 2009.

GAO. *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*. GAO-09-57. Washington, D.C.: January 30, 2009.

GAO. *TSA's Explosives Detection Canine Program: Status of Increasing Number of Explosives Detection Canine Teams.* GAO-08-933R. Washington, D.C.: July 31, 2008.

GAO. *Department of Homeland Security Progress Report on Implementation of Mission and Management Functions*. GAO-07-454. Washington, D.C.: August 17, 2007.

Department of Homeland Security Office of Inspector General, *DHS Grants Used for Mitigating Risks to Amtrak Rail Stations*. OIG-11-93. Washington, D.C.: June 27, 2011.

Department of Homeland Security Office of Inspector General, *Use of American Recovery and Reinvestment Act Funds by the Federal Emergency Management Agency for the Transit Security Grant Program.* OIG-11-18. Washington, D.C.: December 9, 2010.

Border Security

GAO. *Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders*. GAO-11-508T. Washington, D.C.: March 30, 2011.

GAO. *Border Security: Preliminary Observations on the Status of Key Southwest Border Technology Programs.* GAO-11-448T. Washington, D.C.: March 15, 2011.

GAO. *Visa Waiver Program: DHS Has Implemented the Electronic System for Travel Authorization, but Further Steps Needed to Address Potential Program Risks.* GAO-11-335. Washington, D.C.: May 5, 2011.

GAO. *Border Security: DHS's Visa Security Program Needs to Improve Performance Evaluation and Better Address Visa Risk Worldwide*. GAO-11-315. Washington, D.C.: March 31, 2011.

GAO. *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border.* GAO-11-97. Washington, D.C.: December 17, 2010.

GAO. *Secure Border Initiative: DHS Needs to Strengthen Management and Oversight of Its Prime Contractor*. GAO-11-6. Washington, D.C.: October 18, 2010.

GAO. *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options.* GAO-10-860. Washington, D.C.: August 10, 2010.

GAO. *Border Security: CBP Lacks the Data Needed to Assess the FAST Program at U.S. Northern Border Ports*. GAO-10-694. Washington, D.C.: July 19, 2010.

GAO. *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program.* GAO-10-340. Washington, D.C.: May 5, 2010.

GAO. *Secure Border Initiative: DHS Has Faced Challenges Deploying Technology and Fencing Along the Southwest Border*. GAO-10-651T. Washington, D.C.: May 4, 2010.

GAO. *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk.* GAO-10-158. Washington, D.C.: January 29, 2010.

GAO. *Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed*. GAO-10-13. Washington, D.C.: November 19, 2009.

GAO. *Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed.* GAO-09-896. Washington, D.C.: September 9, 2009.

GAO. *Border Patrol: Checkpoints Contribute to Border Patrol's Mission, but More Consistent Data Collection and Performance Measurement*

Could Improve Effectiveness. GAO-09-824. Washington, D.C.: August 31, 2009.

GAO. *Border Security: Despite Progress, Weaknesses in Traveler Inspections Exist at Our Nation's Ports of Entry.* GAO-08-219. Washington, D.C.: November 5, 2007.

Department of Homeland Security Office of Inspector General. *CBP's Efficacy of Controls Over Drug Seizures*. OIG-11-57. Washington, D.C.: March 17, 2011.

Department of Homeland Security Office of Inspector General. *Customs and Border Protection Needs to Improve Its Inspection Procedures for the Western Hemisphere Travel Initiative*. OIG-11-43. Washington, D.C.: February 11, 2011.

Maritime Security

GAO. *Maritime Security: Progress Made but Further Actions Needed to Secure the Maritime Energy Supply.* GAO-11-883T. Washington, D.C.: August 24, 2011.

GAO. *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security*. GAO-11-657. Washington, D.C.: May 10, 2011.

GAO. *Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can be Strengthened*. GAO-11-195. Washington, D.C.: January 14, 2011.

GAO. *Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security*. GAO-11-207. Washington, D.C.: December 3, 2010.

GAO. *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials*. GAO-10-1041T. Washington, D.C.: September 15, 2010

GAO. *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security.* GAO-10-940T. Washington, D.C.: July 21, 2010.

GAO. *Supply Chain Security: DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational*

Scenarios to Ensure the Technologies Will Function as Intended. GAO-10-887. Washington, D.C.: September 29, 2010.

GAO. *Coast Guard: Efforts to Identify Arctic Requirements Are Ongoing, but More Communication about Agency Planning Efforts Would Be Beneficial.* GAO-10-870. Washington, D.C.: September 15, 2010.

GAO. *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*. GAO-10-400. Washington, D.C.: April 9, 2010.

GAO. *Combating Nuclear Smuggling: Recent Testing Raises Issues About the Potential Effectiveness of Advanced Radiation Detection Portal Monitors*. GAO-10-252T. Washington, D.C.: November 17, 2009.

GAO. *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*. GAO-10-12. Washington, D.C.: October 30, 2009.

GAO. *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors*. GAO-09-804T. Washington, D.C.: June 25, 2009.

GAO. *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology.* GAO-09-655. Washington, D.C.: May 21, 2009.

GAO. *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed.* GAO-09-337. Washington, D.C.: March 17, 2009.

GAO. *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*. GAO-08-12. Washington, D.C.: February 14, 2008.

GAO. *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later.* GAO-08-126T. Washington, D.C.: October 30, 2006.

Department of Homeland Security Office of Inspector General. *Customs and Border Protection's Importer Self-Assessment Program*. OIG-10-113. Washington, D.C.: August 30, 2010.

Department of Homeland Security Office of Inspector General. *CBP's Container Security Initiative Has Proactive Management and Oversight but Future Direction Is Uncertain*. OIG-10-52. Washington, D.C.: February 3, 2010.

Department of Homeland Security Office of Inspector General. *Cargo Targeting and Examinations*. OIG-10-34. Washington, D.C.: January 6, 2010.

Department of Homeland Security Office of Inspector General. *CBP's Ability to Detect Biological and Chemical Threats in Maritime Cargo Containers*. OIG-10-01. Washington, D.C.: October 7, 2009.

Immigration Enforcement

GAO. *Overstay Enforcement: Additional Mechanisms for Collecting, Assessing, and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs.* GAO-11-411. Washington, D.C.: April 15, 2011.

GAO. *Employment Verification: Agencies Have Improved E-Verify, but Significant Challenges Remain*. GAO-11-522T. Washington, D.C.: April 14, 2011.

GAO. *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*. GAO-11-146. Washington, D.C.: December 17, 2010.

GAO. *Moving Illegal Proceeds: Challenges Exist in the Federal Government's Effort to Stem Cross-Border Currency Smuggling*, GAO-11-73, Washington, D.C.: October 25, 2010.

GAO. *Alien Smuggling: DHS Needs to Better Leverage Investigative Resources and Measure Program Performance along the Southwest Border*. GAO-10-328. Washington, D.C.: May 24, 2010.

GAO. *Firearms Trafficking: U.S. Efforts to Combat Arms Trafficking to Mexico Face Planning and Coordination Challenges*. GAO-09-709. Washington, D.C.: June 18, 2009.

GAO. *Immigration Enforcement: Better Controls Needed over Program Authorizing State and Local Enforcement of Federal Immigration Laws*. GAO-09-109. Washington, D.C.: January 30, 2009.

Department of Homeland Security Office of Inspector General. *U.S. Immigration and Customs Enforcement Identification of Criminal Aliens in Federal and State Custody Eligible for Removal from the United States*. OIG-11-26. Washington, D.C.: January 10, 2011.

Department of Homeland Security Office of Inspector General. *The Performance of the 287(g) Agreements Report Update*. OIG-10-124. Washington, D.C.: September 30, 2010.

Department of Homeland Security Office of Inspector General. *The Performance of 287(g) Agreements*. OIG-10-63. Washington, D.C.: March 4, 2010.

Immigration Services

GAO. *Immigration Benefits: Actions Needed to Address Vulnerabilities in Process for Granting Permanent Residency.* GAO-09-55. Washington, D.C.: December 5, 2008.

GAO. *U.S. Asylum System: Agencies Have Taken Actions to Help Ensure Quality in the Asylum Adjudication Process, but Challenges Remain*. GAO-08-935. Washington, D.C.: September 25, 2008.

GAO. *Immigration Benefits: Internal Controls for Adjudicating Humanitarian Parole Cases Are Generally Effective, but Some Can Be Strengthened*. GAO-08-282. Washington, D.C.: February 6, 2008.

GAO. *USCIS Transformation: Improvements to Performance, Human Capital and Information Technology Management Needed as Modernization Proceeds*. GAO-07-1013R. Washington, D.C.: July 17, 2007.

Department of Homeland Security Office of Inspector General. *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology*. OIG-09-90. Washington, D.C.: July 13, 2009.

Department of Homeland Security Office of Inspector General. *Management Oversight of Immigration Benefit Application Intake Processes,* OIG-09-37. Washington, D.C.: March 5, 2009.

Department of Homeland Security Office of Inspector General. *Review of the USCIS Benefit Fraud Referral Process,* OIG-08-09. Washington, D.C.: April 29, 2008.

Critical Infrastructure Protection—Cyber Assets

GAO. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*. GAO-11-865T. Washington, D.C.: July, 26, 2011.

GAO. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*. GAO-11-463T. Washington, D.C.: March 16, 2011.

GAO. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*. GAO-10-628. Washington, D.C.: July 15, 2010.

GAO. *Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats*. GAO-10-834T. Washington, D.C.: June 16, 2010.

GAO. *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*. GAO-10-237. Washington, D.C.: March 12, 2010.

GAO. *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*. GAO-10-296. Washington, D.C.: March 5, 2010.

GAO. *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*. GAO-09-969. Washington, D.C.: September 24, 2009.

GAO. *High-Risk Series: An Update*. GAO-09-271. Washington, D.C.: January 2009.

GAO. *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*. GAO-08-825. Washington, D.C.: September 9, 2008.

GAO. *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*. GAO-08-588. Washington, D.C.: July 31, 2008.

Department of Homeland Security Office of Inspector General. *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain*. OIG-10-94. Washington, D.C.: June 7, 2010.

Emergency Preparedness and Response

GAO. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*. GAO-11-865T. Washington, D.C.: July 26, 2011

GAO. *Measuring Disaster Preparedness: FEMA Has Made Limited Progress in Assessing National Capabilities*. GAO-11-260T. Washington, D.C.: March 17, 2011.

GAO. *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*. GAO-11-318SP. Washington, D.C.: March 1, 2011.

GAO. *FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities*. GAO-11-51R. Washington, D.C.: October 29, 2010.

GAO. *Recovery Act: FEMA Could Take Steps to Protect Sensitive Port Security Grant Details and Improve Recipient Reporting Instructions*. GAO-11-88. Washington, D.C.: October 15, 2010.

GAO. *Disaster Recovery: FEMA's Long-term Assistance Was Helpful to State and Local Governments but Had Some Limitations*. GAO-10-404. Washington, D.C.: March 30, 2010.

GAO. *Emergency Communications: Establishment of the Emergency Communications Preparedness Center and Related Interagency Coordination Challenges.* GAO-10-463R. Washington, D.C.: March 3, 2010.

GAO. *Combating Nuclear Terrorism: Actions Needed to Better Prepare to Recover from Possible Attacks Using Radiological or Nuclear Materials.* GAO-10-204. Washington, D.C.: January 29, 2010

GAO*. Combating Nuclear Terrorism: Preliminary Observations on Preparedness to Recovery from Possible Attacks Using Radiological or Nuclear Materials*. GAO-09-996T. Washington, D.C.: September 14, 2009

GAO. *Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System*. GAO-09-834. Washington, D.C.: September 9, 2009.

GAO. *Hurricanes Gustav and Ike Disaster Assistance: FEMA Strengthened Its Fraud Prevention Controls, but Customer Service Needs Improvement*. GAO-09-671. Washington, D.C.: June 19, 2009.

GAO. *Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts*. GAO-09-604. Washington, D.C.: June 19, 2009.

GAO. *National Preparedness: FEMA Has Made Progress, but Needs to Complete and Integrate Planning, Exercise, and Assessment Efforts*. GAO-09-369. Washington, D.C.: April 30, 2009.

GAO. *Disaster Recovery: FEMA's Public Assistance Grant Program Experienced Challenges with Gulf Coast Rebuilding*. GAO-09-129. Washington, D.C.: December 18, 2008.

GAO. *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version's Measure of Vulnerability is Limited*. GAO-08-852. Washington, D.C.: June 27, 2008.

GAO. *National Flood Insurance Program: Financial Challenges Underscore Need for Improved Oversight of Mitigation Programs and Key Contracts*. GAO-08-437. Washington, D.C.: June 16, 2008.

GAO. *National Response Framework: FEMA Needs Policies and Procedures to Better Integrate Non-Federal Stakeholders in the Revision Process*. GAO-08-768. Washington, D.C.: June 11, 2008.

Department of Homeland Security Office of Inspector General. *Efficacy of DHS Grants Programs.* OIG-10-69. Washington, D.C.: March 22, 2010.

DHS Transformation and Implementation

GAO. *High-Risk Series: An Update*. GAO-11-278. Washington, D.C.: February 2011.

GAO. *Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk*. GAO-11-43. Washington, D.C.: November 30, 2010.

GAO. *Department of Homeland Security: Assessments of Selected Complex Acquisitions*. GAO-10-588SP. Washington, D.C.: June 30, 2010.

GAO. *Department of Homeland Security: DHS Needs to Comprehensively Assess Its Foreign Language Needs and Capabilities and Identify Shortfalls*. GAO-10-714. Washington, D.C.: June 22, 2010.

GAO. *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements*. GAO-10-202. Washington, D.C.: March 12, 2010.

GAO. *Financial Management Systems: DHS Faces Challenges to Successfully Consolidating Its Existing Disparate Systems*. GAO-10-76. Washington, D.C.: December 4, 2009.

GAO. *Department of Homeland Security: Actions Taken Toward Management Integration, but a Comprehensive Strategy Is Still Needed*. GAO-10-131. Washington, D.C.: November 20, 2009.

GAO. *Homeland Security: Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems*. GAO-09-1002T. Washington, D.C.: September 15, 2009.

GAO. *Equal Employment Opportunity: DHS Has Opportunities to Better Identify and Address Barriers to EEO in Its Workforce.* GAO-09-639 Washington, D.C.: August 31, 2009.

GAO. *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*. GAO-09-29. Washington, D.C.: November 18, 2008.

GAO. *Department of Homeland Security: Better Planning and Assessment Needed to Improve Outcomes for Complex Service Acquisitions*. GAO-08-263. Washington, D.C.: April 22, 2008.

GAO. *Homeland Security: Departmentwide Integrated Financial Management Systems Remain a Challenge.* GAO-07-536. Washington, D.C.: June 21, 2007.

GAO. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, version 1.1. GAO-04-394G. Washington, D.C.: March 2004.

GAO. *High-Risk Series: Strategic Human Capital Management*. GAO-03-120. Washington, D.C.: January 2003.

GAO. *Determining Performance and Accountability Challenges and High Risks*. GAO-01-159SP. Washington, D.C.: November 2000.

Department of Homeland Security Office of Inspector General. *Major Management Challenges Facing the Department of Homeland Security.* OIG-11-11. Washington, D.C.: November 10, 2010.

Performance Measurement

GAO. *Overstay Enforcement: Additional Mechanisms for Collecting, Assessing, and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs*. GAO-11-411. Washington, D.C.: April 15, 2011.

GAO. *Measuring Disaster Preparedness: FEMA Has Made Limited Progress in Assessing National Capabilities.* GAO-11-260T. Washington, D.C.: March 17, 2011.

GAO. *Department of Homeland Security: Progress Made in Implementation and Transformation of Management Functions, but More Work Remains.* GAO-10-911T. Washington, D.C.: September 30, 2010.

GAO. *Alien Smuggling: DHS Needs to Better Leverage Investigative Resources to Measure Program Performance along the Southwest Border*. GAO-10-328. Washington, D.C.: May 24, 2010.

GAO. *Emergency Preparedness: FEMA Faces Challenges Integrating Community Preparedness Programs into Its Strategic Approach.* GAO-10-193. Washington, D.C.: January 29, 2010.

GAO. *Secure Border Initiative: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed*. GAO-09-1013T. Washington, D.C.: September 17, 2009.

GAO. *Border Patrol: Checkpoints Contribute to Border Patrol's Mission, but More Consistent Data Collection and Performance Measurement Could Improve Effectiveness*. GAO-09-824. Washington, D.C.: August 31, 2009.

GAO. *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*. GAO-07-454. Washington, D.C.: August 17, 2007.

Risk Management

GAO. *National Preparedness: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments*. GAO-11-606. Washington, D.C.: June 21, 2011.

GAO. *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*. GAO-10-867. Washington, D.C.: August 4, 2010.

GAO. *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*. GAO-10-128. Washington, D.C.: October 7, 2009.

GAO. *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*. GAO-09-243. Washington, D.C.: April 21, 2009.

GAO. *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*. GAO-09-492. Washington, D.C.: March 27, 2009.

GAO. *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*. GAO-09-85. Washington, D.C.: February 27, 2009.

GAO. *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*. GAO-09-57. Washington, D.C.: January 30, 2009.

GAO. *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version's Measure of Vulnerability Is Limited*. GAO-08-852. Washington, D.C.: June 27, 2008.

GAO. *Risk Management: Progress Report on Implementation of Mission and Management Functions*. GAO-07-454. Washington, D.C.: August 17, 2007.

GAO. *Department of Homeland Security: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* GAO-06-91. Washington, D.C.: December 15, 2005.

Information Sharing for Homeland Security

GAO. *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*. GAO-11-455. Washington, D.C.: July 21, 2011.

GAO. *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*. GAO-11-688T. Washington, D.C.: June 14, 2011.

GAO. *High-Risk Series: An Update*. GAO-11-278. Washington, D.C.: February 2011.

GAO. *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability.* GAO-11-223. Washington, D.C.: December 16, 2010.

GAO. *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, But Could Better Measure Results*. GAO-10-972. Washington, D.C.: September 29, 2010.

GAO. *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*. GAO-10-895. Washington, D.C.: September 22, 2010.

GAO. *Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Efforts*. GAO-10-650T. Washington, D.C.: April 21, 2010.

Partnerships and Coordination

GAO. *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border*. GAO-11-97. Washington, D.C.: December 17, 2010.

GAO. *Aviation Security: DHS Has Taken Steps to Enhance International Aviation Security and Facilitate Compliance with International Standards, but Challenges Remain*. GAO-11-238T. Washington, D.C.: December 2, 2010.

GAO. *Border Security: Additional Actions Needed to Better Ensure a Coordinated Federal Response to Illegal Activity on Federal Lands*. GAO-11-177. Washington, D.C.: November 18, 2010.

GAO. *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened.* GAO-10-772. Washington, D.C.: September 23, 2010.

GAO. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*. GAO-10-628. Washington, D.C.: July 15, 2010.

GAO. *Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System*. GAO-09-834. Washington, D.C.: September 9, 2009.

GAO, *National Response Framework: FEMA Needs Policies and Procedures to Better Integrate Non-Federal Stakeholders in the Revision Process.* GAO-08-768. Washington, D.C.: June 11, 2008.

GAO. *Homeland Security: Strategic Solution for US-VISIT Program Needs to Be Better Defined, Justified, and Coordinated.* GAO-08-361. Washington, D.C.: February 29, 2008.

GAO. *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions.* GAO-07-454. Washington, D.C.: August 17, 2007.

Developing and Deploying New Technologies for Homeland Security

GAO. *Homeland Security: DHS Could Strengthen Acquisitions and Development of New Technologies.* GAO-11-829T. Washington, D.C.: July 15, 2011.

GAO. *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed*. GAO-11-740. Washington, D.C.: July 11, 2011.

GAO. *DHS Science and Technology: Additional Steps Needed to Ensure Test and Evaluation Requirements Are Met*. GAO-11-596. Washington, D.C.: June 15, 2011.

GAO. *Border Security: Preliminary Observations on the Status of Key Southwest Border Technology Programs*. GAO-11-448T. Washington D.C.: March 15, 2011.

GAO. *Supply Chain Security: DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended*. GAO-10-887. Washington D.C.: September 29, 2010.

GAO. *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials*. GAO-10-1041T. Washington D.C.: September 15, 2010.

GAO. *Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps.* GAO-10-883T. Washington, D.C.: June 30, 2010.

GAO. *Biosurveillance: Efforts to Develop a National Biosurveillance Capability Need A National Strategy and a Designated Leader.* GAO-10-645. Washington, D.C.: June 30, 2010.

GAO. *Combating Nuclear Smuggling: Recent Testing Raises Issues About the Potential Effectiveness of Advanced Radiation Detection Portal Monitors*. GAO-10-252T. Washington, D.C.: November 17, 2009.

GAO. *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors.* GAO-09-804T. Washington, D.C.: June 25, 2009.

GAO. *Combating Nuclear Smuggling: DHS's Program to Procure and Deploy Advanced Radiation Detection Portal Monitors Is Likely to Exceed the Department's Previous Cost Estimates*. GAO-08-1108R. Washington, D.C.: September 22, 2008.

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

Please Print on Recycled Paper