United States Government Accountability Office

Testimony

Before the Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, May 7, 2014

DEPARTMENT OF HOMELAND SECURITY

Progress Made; Significant Work Remains in Addressing High-Risk Areas

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

GAO
Highlights

Highlights of GAO-14-532T, a testimony before the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Since 1990, GAO has regularly reported on government operations identified as high risk because of their greater vulnerability to fraud, waste, abuse, and mismanagement, or the need for transformation to address economy, efficiency, or effectiveness challenges. DHS has sole or critical responsibility for four GAO high-risk areas—(1) strengthening its management functions, (2) NFIP, (3) information security and cyber critical infrastructure protection, and (4) terrorism-related information sharing. This statement addresses DHS's progress and work remaining in addressing high-risk areas for which (1) it has sole responsibility and (2) it has critical, but shared responsibility.

This statement is based on GAO's February 2013 high-risk update, reports and testimonies issued from March 2013 through April 2014, and analyses from GAO's ongoing assessment of DHS's efforts since February 2013 to address its high-risk designations. For these analyses, GAO examined DHS documents and interviewed DHS officials.

What GAO Recommends

This testimony contains no new recommendations. GAO has made over 2,100 recommendations to DHS since its establishment in 2003 to strengthen its management and integration efforts, among other things. DHS has implemented more than 65 percent of these recommendations and has actions under way to address others.

View GAO-14-532T. For more information, contact George A. Scott at (202) 512-8777 or scottg@gao.gov.

May 7, 2014

DEPARTMENT OF HOMELAND SECURITY

Progress Made; Significant Work Remains in Addressing High-Risk Areas

What GAO Found

The Department of Homeland Security (DHS) has made progress in addressing high-risk areas for which it has sole responsibility, but significant work remains.

Strengthening management functions. In this area, DHS has met two and partially met three of GAO's five criteria for removing areas from the high-risk list. Specifically, DHS has met the criteria for having (1) demonstrated leadership commitment, and (2) a corrective action plan for addressing its management risks. However, it has partially met GAO's criteria for (1) capacity (having sufficient resources); (2) having a framework to monitor progress; and (3) demonstrated, sustained progress. DHS has made important progress, but to more fully address GAO's high-risk designation, DHS needs to show measurable, sustainable progress in implementing key management initiatives. For example:

- *Human capital management.* DHS has developed and demonstrated progress in implementing a strategic human capital plan. However, DHS needs to improve other aspects of its human capital management. As GAO reported in December 2013, the Office of Personnel Management's 2013 Federal Employee Viewpoint Survey data showed that DHS ranked 36th of 37 federal agencies in a measure of employee job satisfaction. In addition, employee satisfaction had decreased 7 percentage points since 2011, which is more than the government-wide decrease. Accordingly, DHS has considerable work ahead to improve its employee morale. Further, DHS is finalizing its analysis of skill gaps in key portions of its workforce including emergency management specialists and cyber-focused IT management personnel.
- *Acquisition management.* DHS has made progress in initiating efforts to validate required acquisition documents. However, about half of DHS major programs lack an approved baseline, 77 percent lack approved life cycle cost estimates, and the department has not implemented its acquisition policy consistently. In March 2014, GAO reported that the Transportation Security Administration does not collect or analyze available information that could be used to enhance the effectiveness of its advanced imaging technology. In March 2014, GAO also found that the U.S. Customs and Border Protection (CBP) did not fully follow DHS policy regarding testing for the integrated fixed towers being deployed on the Arizona border. As a result, DHS does not have complete information on how the towers will operate once they are fully deployed.
- *Financial management.* DHS has made progress toward improving its financial management, but a significant amount of work remains to be completed. For example, DHS needs to eliminate all material weaknesses at the department level in areas such as property, plant, and equipment before its financial auditor can assert that the controls are effective. DHS also needs to effectively manage the modernization of financial management systems at the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Federal Emergency Management Agency (FEMA).

- *Information Technology (IT) Management.* While important steps have been taken to define IT investment management processes, work is needed to demonstrate progress in implementing these processes across DHS's 13 IT investment portfolios. In July 2012, GAO recommended that DHS finalize the policies and procedures associated with its new tiered IT governance structure and continue to implement key processes supporting this structure. DHS agreed with these recommendations; however, as of April 2014, the department had not finalized the key IT governance directive, and the draft structure has been implemented across only 5 of the 13 investment portfolios.

National Flood Insurance Program (NFIP). DHS's FEMA, which manages the NFIP, has partially met the five criteria for NFIP removal from the high-risk list, but needs to initiate or complete additional actions. For example, FEMA has not completed actions in certain areas, such as modernizing its claims and policy management system and overseeing compensation of insurers that sell NFIP policies. In addition, FEMA is unlikely to generate sufficient revenue to cover future catastrophic losses or repay billions of dollars borrowed from the Department of the Treasury. As of December 2013, FEMA owed the Treasury $24 billion—primarily to pay claims associated with Superstorm Sandy (2012) and Hurricane Katrina (2005)—and had not made a principal payment since 2010.

Progress has been made in the following government-wide high-risk areas in which DHS plays a critical role, but significant work remains.

Information security and cyber critical infrastructure protection. Federal agencies, including DHS, have taken a variety of actions that were intended to enhance federal and critical infrastructure cybersecurity, but more efforts are needed. DHS needs to take several actions to better oversee and assist agencies in improving information security practices. For instance, DHS should continue to assist agencies in developing and acquiring continuous diagnostic and mitigation capabilities to protect networks and counteract day-to-day cyber threats. In addition, DHS has taken steps to enhance the protection of cyber critical infrastructure but could do more to enhance coordination with the private sector.

Terrorism-related information sharing. The federal government faces significant challenges in sharing terrorism-related information. However, DHS has made significant progress in enhancing the sharing of this information. For example, DHS is taking steps to measure the extent to which fusion centers—collaborative efforts within states that investigate and respond to criminal and terrorist activity—are coordinating with other field-based task forces and centers to share terrorism-related information, and assessing opportunities to improve coordination and information sharing. The federal government has important work ahead to address the high risk issue, such as developing metrics that measure the homeland security results achieved from improved information sharing.

Chairman McCaul, Ranking Member Thompson, and Members of the Committee:

I am pleased to be here today to discuss our work on the Department of Homeland Security's (DHS) ongoing efforts to improve the efficiency of its operations and unity of the department, with a particular focus on DHS's progress and remaining challenges addressing GAO's high-risk designations. In the 11 years since the Department's creation, DHS has implemented key homeland security operations, achieved important goals and milestones, and grown to more than 240,000 employees and approximately $60 billion in budget authority. During that time, our work has identified several areas where DHS needs to address gaps and weaknesses in its current operational and implementation efforts, as well as strengthen the efficiency and effectiveness of those efforts. Since 2003, we have made approximately 2,100 recommendations to DHS to strengthen program management, performance measurement efforts, and management processes, among other things. DHS has implemented more than 65 percent of these recommendations and has actions under way to address others.

We also report regularly to the Congress on government operations that we identified as high risk because of their greater vulnerability to fraud, waste, abuse, and mismanagement, or the need for transformation to address economy, efficiency, or effectiveness challenges. DHS has sole or critical responsibility for four GAO high-risk areas—(1) *Strengthening DHS Management Functions*, (2) *National Flood Insurance Program (NFIP)*, (3) *Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures*, and (4) *Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland*. DHS has made progress addressing areas we have identified as high risk, but needs to continue to strengthen its efforts in order to more efficiently and effectively achieve its homeland security missions. In particular:

- In 2003, we designated implementing and transforming DHS as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to address associated risks could have serious consequences for U.S. national and economic security.[1] While challenges remain across its missions,

[1] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

DHS has made considerable progress in transforming its original component agencies into a single department. As a result, in our 2013 high-risk update, we narrowed the scope of the high-risk area to focus on strengthening DHS management functions (human capital, acquisition, financial management, and information technology [IT]).[2]

- In 2006, we added the NFIP—a key component of the federal government's efforts to limit the damage and financial impact of floods—to the GAO high-risk list because the program faced significant ongoing financial and management challenges.[3] In particular, the NFIP, which is managed by DHS's Federal Emergency Management Agency (FEMA), is unlikely to generate sufficient revenue to cover future catastrophic losses or repay billions of dollars borrowed from the Department of the Treasury to cover insurance claims from previous disasters.

- In 1997, we designated federal information security as a government-wide high-risk area, and we expanded the area in 2003 to include systems supporting critical infrastructure such as power distribution, communications, banking and finance, water supply, national defense, and emergency services.[4] The effective security of these systems and the data they contain is essential to national security, economic well-being, and public health and safety. DHS is responsible for securing its own information systems and data and also plays a pivotal role in government-wide cybersecurity efforts.

- In 2005, we designated the sharing of terrorism-related information as high risk because of the significant challenges the federal government faces in sharing this information in a timely, accurate, and useful manner.[5] The sharing of terrorism-related information is a government-wide effort that involves numerous federal departments and agencies. DHS plays a critical role in this sharing given its homeland security missions and responsibilities.

[2] GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013). For additional information, see our high risk list key issues page at http://www.gao.gov/highrisk/overview.

[3] GAO, *GAO's High-Risk Program*, GAO-06-497T (Washington, D.C.: Mar. 15, 2006).

[4] GAO-03-119.

[5] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 1, 2005).

In November 2000, we published our criteria for removing areas from the high-risk list.[6] Specifically, agencies must have (1) a demonstrated strong commitment and top leadership support to address the risks; (2) a corrective action plan that identifies the root causes, identifies effective solutions, and provides for substantially completing corrective measures in the near term, including but not limited to steps necessary to implement solutions we recommended; (3) the capacity (that is, the people and other resources) to resolve the risks; (4) a program instituted to monitor and independently validate the effectiveness and sustainability of corrective measures; and (5) the ability to demonstrate progress in implementing corrective measures. When legislative, administration, and agency actions, including those in response to our recommendations, result in significant progress toward resolving a high-risk problem, we remove the high-risk area.

My testimony today discusses our observations on DHS's progress and work remaining in addressing (1) high-risk areas for which DHS has sole responsibility, and (2) high-risk areas for which DHS has critical, but shared, responsibility.

This statement is based on GAO's 2013 high-risk update as well as reports and testimonies we issued from March 2013 through April 2014.[7] For the past products, among other things, we analyzed DHS strategies and other documents related to the department's efforts to address its high-risk areas; reviewed our past reports issued since DHS began its operations in March 2003; and interviewed DHS officials. More detailed information on the scope and methodology of our prior work can be found within each specific report. This statement is also based on analyses from our ongoing assessment of DHS's efforts to address its high-risk areas since February 2013. We expect to report final results from this work in our 2015 high-risk update. For our analyses, among other things, we analyzed DHS documentation, such as departmental guidance, and met with DHS officials, including the Deputy Secretary and Under Secretary for Management, to discuss DHS's efforts to address its high-risk areas. With respect to the *Strengthening DHS Management Functions* high-risk area, on May 1, 2014, DHS provided us with an updated version of its

[6] GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: Nov. 1, 2000).

[7] GAO-13-283.

Integrated Strategy for High Risk Management. We plan to analyze this update as part of our ongoing assessment of DHS's progress in addressing this high-risk area.

We conducted the work on which this statement is based 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.

High-Risk Areas for Which DHS Has Sole Responsibility

DHS has made progress in addressing high-risk areas for which it has sole responsibility, but significant work remains.

Strengthening DHS Management Functions

DHS has made important progress in implementing, transforming, strengthening, and integrating its management functions in human capital, acquisition, financial management, and IT. This has included taking numerous actions specifically designed to address our criteria for removing areas from the high-risk list. However, as we reported in our February 2013 high risk update, this area remains high risk because the department has significant work ahead.[8] As shown in table 1, DHS has met two of our criteria for removal from the high-risk list (leadership commitment and a corrective action plan), and has partially met the remaining three criteria (a framework to monitor progress; capacity; and demonstrated, sustained progress).

[8] GAO-13-283.

Table 1: Assessment of Department of Homeland Security (DHS) Progress in Addressing the Strengthening DHS Management Functions High-Risk Area, as of May 2014

Criterion for removal from the high-risk list	Met[a]	Partially met[b]	Not met[c]
Leadership commitment	X		
Corrective action plan	X		
Capacity		X	
Framework to monitor progress		X	
Demonstrated, sustained progress		X	
Total	**2**	**3**	**0**

Source: GAO analysis of DHS documents, interviews, and prior GAO reports.

[a] "Met": There are no significant actions that need to be taken to further address this criterion.

[b] "Partially met": Some but not all actions necessary to generally meet the criterion have been taken.

[c] "Not met": Few, if any, actions toward meeting the criterion have been taken.

Leadership commitment (met). The Secretary and Deputy Secretary of Homeland Security, the Under Secretary for Management at DHS, and other senior officials have continued to demonstrate commitment and top leadership support for addressing the department's management challenges. They have also taken actions to institutionalize this commitment to help ensure the long-term success of the department's efforts. For example, in May 2012, the Secretary of Homeland Security modified the delegations of authority between the Management Directorate and its counterparts at the component level to clarify and strengthen the authorities of the Under Secretary for Management across the department.

In addition, in April 2014, the Secretary of Homeland Security issued a memorandum committing to improving DHS's planning, programming, budgeting, and execution processes through strengthened departmental structures and increased capability. This memorandum identified several initial areas of focus intended to build organizational capacity.[9] Senior DHS officials have also routinely met with us over the past 5 years to discuss the department's plans and progress in addressing this high-risk area, during which we provided specific feedback on the department's efforts. According to these officials, and as demonstrated through their progress, the department is committed to demonstrating measurable,

[9] DHS, Secretary of Homeland Security, *Strengthening Departmental Unity of Effort,* Memorandum for DHS Leadership (Washington, D.C.: April *22,* 2014).

sustained progress in addressing this high-risk area. It will be important for DHS to maintain its current level of top leadership support and sustained commitment to ensure continued progress in successfully executing its corrective actions through completion.

Corrective action plan (met). DHS established a plan for addressing this high-risk area. In a September 2010 letter to DHS, we identified and DHS agreed to achieve 31 actions and outcomes that are critical to addressing the challenges within the department's management areas and in integrating those functions across the department. In January 2011, DHS issued its initial *Integrated Strategy for High Risk Management,* which included key management initiatives and related corrective action plans for addressing its management challenges and the outcomes we identified. DHS provided updates of its progress in implementing these initiatives and corrective actions in its later versions of the strategy. In March 2014, we made updates to the actions and outcomes in collaboration with DHS to reduce overlap and ensure their continued relevance and appropriateness. These updates resulted in a reduction from 31 to 30 total actions and outcomes.

DHS's strategy and approach to continuously refining actionable steps to implementing the outcomes, if implemented effectively and sustained, provide a path for DHS to be removed from GAO's high-risk list.

Capacity (partially met). In May 2014, DHS identified that it had resources needed to implement 7 of the 11 initiatives the department had under way to address the actions and outcomes, but did not identify sufficient resource needs for the 4 remaining initiatives. In our analysis of DHS's June 2013 update, which similarly did not identify sufficient resource needs for all initiatives, we found that this absence of complete resource information made it difficult to fully assess the extent to which DHS has the capacity to implement its initiatives.

In addition, our prior work has identified specific capacity gaps that could undermine achievement of management outcomes. For example, in September 2012, we reported that 51 of 62 acquisition programs faced workforce shortfalls in program management, cost estimating, engineering, and other areas, increasing the likelihood that the programs will perform poorly in the future.[10] Since that time, DHS has appointed component acquisition executives at the components and made progress in filling staff positions. In April 2014, however, we reported that DHS needed to increase its cost-estimating capacity, and that the department had not approved baselines for 21 of 46 major acquisition programs.[11] These baselines—which establish cost, schedule, and capability parameters—are necessary to accurately assess program performance.

DHS needs to continue to identify resources for the remaining initiatives; determine that sufficient resources and staff are committed to initiatives; work to mitigate shortfalls and prioritize initiatives, as needed; and communicate to senior leadership critical resource gaps.

Framework to monitor progress (partially met). DHS established a framework for monitoring its progress in implementing the corrective actions it identified for addressing the 30 actions and outcomes. In the June 2012 update to the *Integrated Strategy for High Risk Management*, DHS included, for the first time, performance measures to track its progress in implementing all of its key management initiatives. DHS continued to include performance measures in its May 2014 update.

Additionally, in March 2014, the Deputy Secretary began meeting monthly with the DHS management team to discuss DHS's progress in strengthening its management functions. According to senior DHS officials, as part of these meetings, attendees discuss a report that senior DHS officials update each month, which identifies corrective actions for each outcome, as well as projected and actual completion dates.

However, there are opportunities for DHS to strengthen this framework. For example, as we reported in September 2013, DHS components need to develop performance and functionality targets for assessing their proposed financial systems.[12] This would include having an independent

[10] GAO, *Homeland Security: DHS Requires More Disciplined Investment Management to Help Meet Mission Needs*, GAO-12-833. (Washington, D.C.: Sept. 18, 2012).

[11] GAO, *Homeland Security Acquisitions: DHS Could Better Manage Its Portfolio to Address Funding Gaps and Improve Communications with Congress*, GAO-14-332 (Washington, D.C.: Apr. 17, 2014).

[12] GAO, *DHS Financial Management: Additional Efforts Needed to Resolve Deficiencies in Internal Controls and Financial Management Systems*, GAO-13-561 (Washington, D.C.: Sept. 30, 2013).

validation and verification program in place to ensure the modernized financial systems meet expected targets. Moving forward, DHS will need to closely track and independently validate the effectiveness and sustainability of its corrective actions and make midcourse adjustments, as needed.

Demonstrated, sustained progress (partially met). Key to addressing the department's management challenges is DHS demonstrating the ability to achieve sustained progress across the 30 actions and outcomes we identified and DHS agreed were needed to address the high-risk area. These actions and outcomes include, among others, validating required acquisition documents in accordance with a department-approved, knowledge-based acquisition process, and sustaining clean audit opinions for at least 2 consecutive years on department-wide financial statements and internal controls. As illustrated by the examples below, DHS has made important progress in implementing corrective actions across its management functions, but it has not demonstrated sustainable, measurable progress in addressing key challenges that remain within these functions and in the integration of those functions.[13]

Human capital management. DHS has mostly addressed one of the seven human capital management outcomes and partially addressed the remaining six. For example, as we reported in December 2012, DHS has developed and demonstrated progress in implementing a strategic human capital plan.[14] This plan, among other things, is integrated with broader organizational strategic planning, and mostly addresses this outcome. However, DHS needs to improve other aspects of its human capital management. For example:

- As we reported in December 2013, the Office of Personnel Management's 2013 Federal Employee Viewpoint Survey data showed that DHS employee satisfaction was 36th of 37 federal agencies and had decreased 7 percentage points since 2011, which

[13] For our assessments of DHS's progress in addressing the 30 outcomes, "fully addressed" means the outcome is fully addressed; "mostly addressed" means progress is significant and a small amount of work remains; "partially addressed" means progress is measurable, but significant work remains; and "initiated" means activities have been initiated to address outcomes, but it is too early to report progress.

[14] GAO, *DHS Strategic Workforce Planning: Oversight of Departmentwide Efforts Should Be Strengthened*, GAO-13-65 (Washington, D.C.: Dec. 3, 2012).

is more than the government-wide decrease of 4 percentage points over the same time period.[15] As a result, the gap between average DHS employee satisfaction and the government-wide average widened to 7 percentage points.[16] Accordingly, DHS has considerable work ahead to improve its employee morale.

- Further, according to senior DHS officials, the department has efforts under way intended to link workforce planning efforts to strategic and program-specific planning efforts to identify current and future human capital needs, including the knowledge, skills, and abilities needed for the department to meet its goals and objectives. According to these officials, the department is in the process of finalizing competency gap assessments to identify potential skills gaps within its components that collectively encompass almost half of the department's workforce. These assessments focus on occupations DHS identifies as critical to its mission, including emergency management specialists and cyber-focused IT management personnel. DHS plans to analyze the results of these assessments and develop plans to address any gaps the assessments identify by the end of fiscal year 2014. This is a positive step, as identifying skills gaps could help the department to better identify current and future human capital needs and ensure the department possesses the knowledge, skills, and abilities needed to meet its goals and objectives. Given that DHS is finalizing these assessments, it is too early to assess their effectiveness.

Acquisition management. DHS has mostly addressed one of the five acquisition management outcomes, partially addressed one, and initiated activities to address the remaining three. DHS has made the most progress in increasing component-level acquisition capability by, for example, establishing a component acquisition executive in each DHS component to provide oversight and support programs within its portfolio. DHS has also taken steps to enhance its acquisition workforce by establishing centers of excellence for cost estimating, systems engineering, and other disciplines to promote best practices and provide

[15] The Federal Employee Viewpoint Survey measures employees' perceptions of whether and to what extent conditions characterizing successful organizations are present in their agencies.

[16] GAO, *Department of Homeland Security: DHS's Efforts to Improve Employee Morale and Fill Senior Leadership Vacancies*, GAO-14-228T. (Washington, D.C.: Dec. 12, 2013).

technical guidance. However, DHS needs to improve its acquisition management. For example:

- DHS initiated a governance body in 2013 to review and validate acquisition programs' requirements and identify and eliminate any unintended redundancies, but it considered trade-offs only across acquisition programs within the department's cybersecurity portfolio. DHS acknowledged that the department has no formal structure in place to consider trade-offs DHS-wide, but DHS anticipates chartering such a body by the end of May 2014.

- DHS also has initiated efforts to validate required acquisition documents in accordance with a knowledge-based acquisition process, but this remains a major challenge for the department. A knowledge-based approach provides developers with information needed to make sound investment decisions, and it would help DHS address significant challenges we have identified across its acquisition programs.[17] DHS's acquisition policy largely reflects key acquisition management practices, but the department has not implemented it consistently. In March 2014, we reported that the Transportation Security Administration does not collect or analyze available information that could be used to enhance the effectiveness of its advanced imaging technology.[18] In March 2014, we also found that U.S. Customs and Border Protection (CBP) did not fully follow DHS policy regarding testing for the integrated fixed towers being deployed on the Arizona border.[19] As a result, DHS does not have complete information on how the towers will operate once they are fully deployed.

- Finally, DHS does not have the acquisition management tools in place to consistently demonstrate whether its major acquisition programs

[17] In our past work examining weapon acquisition issues and best practices for product development, we have found that leading commercial firms pursue an acquisition approach that is anchored in knowledge, whereby high levels of product knowledge are demonstrated by critical points in the acquisition process.

[18] GAO, *Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems*, GAO-14-357 (Washington, D.C.: March 31, 2014).

[19] GAO, *Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness*, GAO-14-368 (Washington, D.C.: Mar. 3, 2014).

are on track to achieve their cost, schedule, and capability goals. About half of major programs lack an approved baseline, and 77 percent lack approved life cycle cost estimates. DHS stated in its 2014 update that it will take time to demonstrate substantive progress in this area. We have recently initiated two reviews to examine DHS's progress in these high-risk areas. In addition, the House Homeland Security committee recently introduced a DHS acquisition reform bill that reinforces the importance of key acquisition management practices, such as establishing cost, schedule, and capability parameters, and includes requirements to better identify and address poor-performing acquisition programs, which could aid the Department in addressing its acquisition management challenges.

Financial management: DHS has made progress toward improving its financial management and has fully addressed one of eight high-risk financial management outcomes—ensuring its financial statements are accurate and reliable.[20] However, a significant amount of work remains to be completed on the other seven outcomes related to DHS's financial statements, internal control over financial reporting, and modernizing financial management systems.

- DHS produced accurate and reliable financial statements for the first time in fiscal year 2013, in part through management's commitment to improving its financial management process. As of May 2014, DHS is working toward sustaining this key achievement.

- DHS has also made some progress toward implementing effective internal control over financial reporting, in part by implementing a corrective action planning process aimed at addressing internal control weaknesses. For example, the department took corrective actions to reduce the material weakness in environmental and other

[20] The financial management outcomes have twice been revised since September 2010 when they were initially established. The most recent revision occurred in March 2014 when GAO and DHS agreed to revise the outcomes to clarify certain requirements and eliminate overlap among the outcomes and between the outcomes and GAO's high risk removal criteria.

liabilities to a significant deficiency.[21] However, DHS needs to eliminate all material weaknesses at the department level before its financial auditor can assert that the controls are effective. For example, one of the material weaknesses involves deficiencies in property, plant, and equipment. DHS plans to achieve this outcome for fiscal year 2016. To meet another outcome, DHS needs to sustain these efforts for 2 years.

- DHS also needs to effectively manage the modernization of financial management systems at the U.S. Coast Guard (USCG), U.S. Immigration and Customs Enforcement (ICE), and the Federal Emergency Management Agency (FEMA). Both USCG and ICE have made some progress toward modernizing their systems and foresee moving to a federal shared service provider and completing their efforts in the latter part of 2016 and 2017.[22] Because of critical stability issues with its legacy financial system that were resolved in May 2013, FEMA postponed its modernization efforts and has not restarted them.

IT Management. DHS has fully addressed one of the six IT management outcomes and partially addressed the remaining five. In particular, the department has strengthened its enterprise architecture program (or blueprint) to guide IT acquisitions by, among other things, largely addressing our prior recommendations aimed at adding needed architectural depth and breadth, thus fully addressing this outcome. However, the department needs to continue to demonstrate progress in strengthening other core IT management areas. For example,

- While the department is taking the necessary steps to enhance its IT security program, such as finalizing its annual Information Security Performance Plan, further work will be needed for DHS to eliminate

[21] Environmental liabilities consist of environmental remediation, cleanup, and decommissioning. A significant deficiency is a deficiency, or combination of deficiencies, in internal control important enough to merit attention by those charged with governance. 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.

[22] A shared service provider is a third-party entity that manages and distributes software-based services and solutions to customers across a wide area network from a central data center.

the department's current material weakness in its information security. It will be important for the department to fully implement its plan, since DHS's financial statement auditor reported in December 2013 that flaws in the security controls such as access controls, contingency planning, and segregation of duties were a material weakness for financial reporting purposes.

- While important steps have been taken to define IT investment management processes generally consistent with best practices, work is needed to demonstrate progress in implementing these processes across DHS's 13 IT investment portfolios.[23] In July 2012, we recommended that DHS finalize the policies and procedures associated with its new tiered IT governance structure and continue to implement key processes supporting this structure.[24] DHS agreed with these recommendations; however, as of April 2014, the department had not finalized the key IT governance directive, and the draft structure has been implemented across only 5 of the 13 investment portfolios.[25]

Fully addressing these actions would also help DHS to address key IT operations efficiency initiatives, as well as to more systematically identify other opportunities for savings. For example, as part of the Office of Management and Budget's data center consolidation initiative, we reported that DHS planned to consolidate from 101 data centers to 37 data centers by December 2015.[26] Further, DHS officials told us that the department had achieved actual cost savings totaling about $140 million in fiscal years 2011 through 2013, and that it estimates total consolidation cost savings of approximately $650 million through fiscal year 2019.

[23] The 13 portfolios are intelligence, domain awareness, securing, screening, law enforcement, information sharing and safeguarding, continuity-of-operations planning, benefits administration, incident management, enterprise business services, enterprise financial management, enterprise IT services, and enterprise human capital.

[24] GAO, *Information Technology: DHS Needs to Further Define and Implement Its New Governance Process*, GAO-12-818 (Washington, D.C.: July 25, 2012).

[25] The draft structure has been implemented across the following five portfolios: intelligence, screening, information sharing and safeguarding, enterprise IT services, and enterprise human capital.

[26] GAO, *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed*, GAO-12-742 (Washington, D.C.: July 19, 2012).

- DHS has also made progress in establishing and implementing sound IT system acquisition processes, but continued efforts are needed to ensure that the department's major IT acquisition programs are applying these processes and obtaining more predictable outcomes. In 2013, DHS's Office of the Chief Information Officer led an assessment of its major IT programs (against industry best practices in key IT system acquisition process areas) to determine its capability strengths and weaknesses, and has work under way to track programs' progress in addressing identified capability gaps, such as requirements management and risk analysis. While this gap analysis and approach for tracking implementation of corrective actions are important steps, DHS will need to show that these actions are resulting in better, more predictable outcomes for its major IT system acquisitions. Demonstrated progress in closing these gaps is especially important in light of our recent reports on major DHS IT programs experiencing significant challenges largely because of system acquisition process shortfalls, including DHS's major border security system modernization, known as TECS-Mod.[27]

Management integration. DHS has made substantial progress integrating its management functions, fully addressing three of the four outcomes we identified as key to the department's management integration efforts. For example, DHS issued a comprehensive plan to guide its management integration efforts—the *Integrated Strategy for High Risk Management*—in January 2011, and has generally improved upon this plan with each update. In addition, in April 2014, the Secretary of Homeland Security issued a memorandum committing to improving DHS's planning, programming, budgeting, and execution processes through strengthened departmental structures and increased capability.[28] To achieve the last and most significant outcome—implement actions and outcomes in each management area to develop consistent or consolidated processes and systems within and across its management functional areas—DHS needs to continue to demonstrate sustainable progress integrating its management functions within and across the department and its components and take additional actions to further and more effectively integrate the department.

[27] GAO, *Border Security: DHS's Efforts to Modernize Key Enforcement Systems Could be Strengthened,* GAO-14-62 (Washington, D.C.: Dec. 5, 2013).

[28] DHS, Secretary of Homeland Security, *Strengthening Departmental Unity of Effort,* Memorandum for DHS Leadership (Washington, D.C.; April *22,* 2014).

For example, recognizing the need to better integrate its lines of business, in February 2013, the Secretary of Homeland Security signed a policy directive establishing the principles of the Integrated Investment Life Cycle Management to guide planning, executing, and managing critical investments department-wide. DHS's June 2013 *Integrated Strategy for High Risk Management* identified that Integrated Investment Life Cycle Management will require significant changes to DHS planning, executing, and managing critical investments. At that time, DHS was piloting elements of the framework to inform a portion of the fiscal year 2015 budget. DHS's May 2014 strategy update states that the department plans to receive an independent analysis of the pilots in May 2014. Given that these efforts are under way, it is too early to assess their impact.

As we reported in March 2013, to more fully address the *Strengthening DHS Management Functions* high-risk area, DHS needs to continue implementing its *Integrated Strategy for High Risk Management* and show measurable, sustainable progress in implementing its key management initiatives and corrective actions and achieving outcomes.[29] In doing so, it will be important for DHS to

- maintain its current level of top leadership support and sustained commitment to ensure continued progress in executing its corrective actions through completion;
- continue to implement its plan for addressing this high-risk area and periodically report its progress to Congress and GAO;
- monitor the effectiveness of its efforts to establish reliable resource estimates at the department and component levels, address and work to mitigate any resource gaps, and prioritize initiatives as needed to ensure it has the capacity to implement and sustain its corrective actions;
- closely track and independently validate the effectiveness and sustainability of its corrective actions and make midcourse adjustments, as needed; and
- make continued progress in addressing the 30 actions and outcomes—for the majority of which significant work remains—and demonstrate that systems, personnel, and policies are in place to ensure that progress can be sustained over time.[30]

[29] GAO, *High-Risk Series, Government-wide 2013 Update and Progress Made by the Department of Homeland Security*, GAO-13-444T (Washington, D.C.: March 21, 2013).

[30] GAO-13-444T.

We will continue to monitor DHS's efforts in this high-risk area to determine if the actions and outcomes are achieved and sustained.

National Flood Insurance Program

FEMA has made progress in all of the areas required for removal of the NFIP from the high-risk list, but needs to initiate or complete additional actions; also, recent legislation has created challenges for FEMA in addressing the financial exposure created by the program. FEMA leadership has displayed a commitment to addressing these challenges and has made progress in a number of areas, such as financial reporting and continuity planning. While FEMA has plans for addressing and tracking progress on our specific recommendations, it has yet to address many of them. For example, FEMA has not completed actions in certain areas, such as modernizing its claims and policy management system and overseeing compensation of insurers that sell NFIP policies. Completing such actions will likely help improve the financial stability and operations of the program. Table 2 summarizes DHS's progress in addressing the NFIP high-risk area.

Table 2: Assessment of Department of Homeland Security Progress in Addressing the National Flood Insurance Program High-Risk Area, as of May 2014

Criterion for removal from the high-risk list	Met[a]	Partially met[b]	Not met[c]
Leadership commitment		x	
Corrective action plan		x	
Capacity		x	
Framework to monitor progress		x	
Demonstrated, sustained progress		x	
Total	**0**	**5**	**0**

Source: GAO analysis of Federal Emergency Management Agency documents, interviews, and prior GAO reports.

[a] "Met": There are no significant actions that need to be taken to further address this criterion.

[b] "Partially met": Some but not all actions necessary to generally meet the criterion have been taken.

[c] "Not met": Few, if any, actions toward meeting the criterion have been taken.

Leadership commitment (partially met). FEMA officials responsible for the NFIP have shown a commitment to taking a number of actions to implement our recommendations, which are designed to improve both the financial stability and operations of the program. For example, they have indicated a commitment to implementing our recommendations and have been proactive in clarifying and taking the actions needed to do so. In addition, FEMA officials have met with us to discuss outstanding recommendations, the actions they have taken to address them, and additional actions they could take. Further, a DHS official said that FEMA holds regular meetings to discuss the status of open recommendations.

Recent legislative changes, however, have presented challenges for FEMA in addressing the financial exposure created by the NFIP. For example, in July 2012, the Biggert-Waters Flood Insurance Reform Act of 2012 (Biggert-Waters Act) was enacted, containing provisions to help strengthen the future financial solvency and administrative efficiency of NFIP, including phasing out almost all discounted insurance premiums (commonly referred to as subsidized premiums).[31] In July 2013, we reported that FEMA was starting to implement some of the required changes.[32] However, on March 21, 2014, the Homeowner Flood Insurance Affordability Act of 2014 (2014 Act) was enacted, reinstating certain premium subsidies and restoring grandfathered rates removed by the Biggert-Waters Act.[33] The 2014 Act addresses affordability concerns for certain property owners, but may also increase NFIP's long-term financial burden on taxpayers.[34]

Corrective action plan (partially met). While FEMA developed corrective action plans for implementing the recommendations in individual GAO reports, it has not developed a comprehensive plan to address the issues that have placed the NFIP on GAO's high-risk list. While addressing our recommendations is part of such a plan, a comprehensive plan also defines the root causes, identifies effective solutions, and provides for substantially completing corrective measures near term. According to a DHS official, the individual action plans collectively represent their plan for addressing these issues, as the recommendations cover steps needed to improve the program's financial stability as well as its administration. The official added that DHS has developed more comprehensive plans for other high-risk areas, which have been helpful, and could consider doing so for the NFIP, but such plans require a lot of work. Such a plan could help FEMA ensure that all

[31] Pub. L. No. 112-141, Div. F, Title II, Subtit. A, 126 Stat. 405, 916 (July 6, 2012).

[32] GAO, *Flood Insurance: More Information Needed on Subsidized Properties*,GAO-13-607 (Washington, D.C.: July 3, 2013).

[33] Pub. L. No. 113-89, 128 Stat. 1020 (Mar. 21, 2014).

[34] GAO, *Flood Insurance: Strategies for Increasing Private Sector Involvement,* GAO-14-127 (Washington, D.C.: Jan. 22, 2014).

important issues, and all aspects of those issues, are addressed. For example, while our recommendations regarding the NFIP's financial stability have focused on the extent of subsidized rates and the rate-setting process, financial stability could include other important areas, such as debt management. As of December 2013, FEMA owed the Treasury $24 billion—primarily to pay claims associated with Superstorm Sandy (2012) and Hurricane Katrina (2005)—and had not made a principal payment since 2010.

Capacity (partially met). FEMA faces several challenges in improving the program's financial stability and operations. First, recent legislative changes permit certain premium subsidies and restore grandfathered rates removed by the Biggert-Waters Act. These provisions, along with others, may weaken the potential for improved financial soundness of the NFIP program. Second, while FEMA is establishing a reserve fund as required by the Biggert-Waters Act, it is unlikely to initially meet the act's annual targets for building up the reserve, partly because of statutory limitations on annual premium increases. Third, while FEMA has begun taking some actions to improve its administration of the NFIP, it is unclear how the resources required to implement both the Biggert-Waters Act and the 2014 Act will affect its ability to continue and complete these efforts. For example, the Acts require FEMA to complete multiple studies and take a number of actions within the next several years, which will require resources FEMA would normally have committed to other efforts.

Monitoring Progress (partially met). FEMA has a process in place to monitor progress in taking actions to implement our recommendations related to the NFIP. For example, the status of efforts to address the recommendations is regularly discussed both within the Flood Insurance and Mitigation Administration, which administers the NFIP, and at the DHS level, according to a DHS official. However, it does not have a specific process for independently validating the effectiveness or sustainability of those actions. Instead, according to a DHS official, once a recommendation related to the NFIP is implemented, the effects of the actions taken to do so are not tracked separately, but are evaluated as part of regular reviews of the effectiveness of the entire program. Broader monitoring of the effectiveness and sustainability of its actions would help ensure that appropriate corrective actions are being taken.

Demonstrated, sustained progress (partially met). FEMA has begun to take actions to improve the program's financial stability, such as initiating actions to improve the accuracy of full-risk rates.[35] However, these efforts are not complete, and FEMA does not have some information, such as the number and location of existing grandfathered properties and information necessary to appropriately revise premium rates for previously subsidized properties.[36] Similarly, FEMA has taken a number of actions to improve areas of the program's operations, such as financial reporting and continuity planning.[37] However, some important actions, such as modernizing its policy and claims management system and ensuring the reasonableness of compensation to insurance companies that sell and service most NFIP policies, remain to be completed.[38] Sustained progress will be needed for FEMA to address the financial and operational issues facing NFIP.

Government-wide High-Risk Areas in Which DHS Plays a Critical Role

Progress has been made in the government-wide high-risk areas in which DHS plays a critical role, but significant work remains.

Information Security and Cyber Critical Infrastructure Protection

As we reported in our February 2013 high-risk update, the White House and federal agencies, including DHS, have taken a variety of actions that were intended to enhance federal and critical infrastructure cybersecurity. For example, the government issued numerous strategy-related documents over the past decade and established agency performance goals and a mechanism to monitor performance in three cross-agency

[35] GAO, *Flood Insurance*: *FEMA's Rate-Setting Process Warrants Attention*, GAO-09-12 (Washington, D.C.: Oct. 31, 2008).

[36] GAO-13-607.

[37] GAO, *FEMA: Action Needed to Improve Administration of the National Flood Insurance Program,* GAO-11-297 (Washington, D.C.: June 9, 2011).

[38] GAO, *Flood Insurance: Opportunities Exist to Improve Oversight of the WYO Program*, GAO-09-455 (Washington, D.C.: Aug. 21, 2009) and GAO-11-297.

priority areas of strong authentication, Trusted Internet Connections, and continuous monitoring.[39]

In addition, since the February 2013 high-risk update, the administration has continued its cyber-related efforts. In February 2013, the President issued Presidential Policy Directive 21 on critical infrastructure security and resilience[40] and Executive Order 13636 on improving critical infrastructure cybersecurity.[41] These documents assign specific actions to particular individuals and agencies with specific time frames for completion.

However, more efforts are needed by federal organizations, including the White House, DHS, and other agencies, to address a number of areas. To illustrate the scope and persistence of this challenge, in fiscal year 2013, inspectors general at 21 of the 24 agencies cited information security as a major management challenge for their agencies,[42] and 18 agencies reported that information security control deficiencies were

[39] Strong authentication involves increasing the use of federal smartcard credentials such as Personal Identity Verification and Common Access Cards that provide multifactor authentication and digital signature and encryption capabilities, authorizing users to access federal information systems with a higher level of assurance. Trusted Internet Connections is an initiative to consolidate external telecommunication connections and ensure a set of baseline security capabilities for situational awareness and enhanced monitoring. Continuous monitoring of federal information systems includes transforming the otherwise static security control assessment and authorization process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk management decisions based on increased situational awareness.

[40] The White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013).

[41] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[42] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development .

either a material weakness or a significant deficiency in internal controls over financial reporting in fiscal year 2013.[43]

DHS's Role in Federal Information Security and Cyber Critical Infrastructure Protection

In addition to having responsibilities for securing its own information systems and data, DHS plays a pivotal role in government-wide cybersecurity efforts. In particular, in July 2010, the Director of the Office of Management and Budget (OMB) and the White House Cybersecurity Coordinator issued a joint memorandum that transferred several key OMB responsibilities under the Federal Information Security Management Act of 2002 (FISMA) to DHS.[44] Specifically, DHS is to exercise primary responsibility within the executive branch for overseeing and assisting with the operational aspects of cybersecurity for federal systems that fall within the scope of FISMA.

We agree that DHS should play a role in the operational aspects of federal cybersecurity. We suggested in February 2013 that Congress consider legislation that would clarify roles and responsibilities for implementing and overseeing federal information security programs and for protecting the nation's critical cyber assets.[45]

Regarding cyber critical infrastructure protection, a fundamental component of DHS's efforts is its partnership approach, whereby it engages in partnerships among government and industry stakeholders. Such an approach is essential because the majority of critical infrastructure in the United States is owned and operated by the private sector. In 2006, DHS issued the National Infrastructure Protection Plan. The plan, subsequently updated several times, provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.[46] Congress is considering several bills that would address cyber information sharing and the

[43] A control deficiency 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.

[44] See Pub. L. No. 107-347, Dec. 17, 2002; 44 U.S.C. 3541, et seq.

[45] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[46] See, most recently, Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.*

cybersecurity posture of the federal government and the nation. For example, H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014, would address DHS's role and responsibilities in protecting federal civilian information systems and critical infrastructure from cyber threats.[47]

Specific laws, executive orders, and directives have further guided DHS's role in cyber critical infrastructure protection. For example, Executive Order 13636 directs DHS to, among other things, establish a voluntary program to support the adoption of a cybersecurity framework by private-sector partners;[48] coordinate the establishment of a set of incentives designed to promote participation in the voluntary program; and incorporate privacy and civil liberties protections into every initiative called for by the executive order.

Securing Federal Systems

In carrying out its role in overseeing and assisting federal agencies in implementing information security requirements, DHS has begun performing several activities. These include

- conducting "CyberStat" reviews, which are intended to hold agencies accountable and offer assistance in improving their information security posture;
- holding interviews with agency chief information officers and chief information security officers on security status and issues;
- establishing a program to enable federal agencies to expand their continuous diagnostics and mitigation capabilities; and
- refining performance metrics that agencies use for FISMA reporting purposes.

In February 2014, as part of our continued dialogue with DHS regarding progress and what remains to be accomplished in this high-risk area, we identified and communicated to DHS actions critical to addressing its

[47] H.R. 3696, 113th Cong. (2013).

[48] As required by Executive Order 13636, the National Institute of Standards and Technology (NIST) issued the first version of the cybersecurity framework in February 2014. See NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Feb. 12, 2014).

efforts to oversee and assist agencies in improving information security practices.[49] This included the following:

- **Expand CyberStat reviews to all major federal agencies.** DHS has conducted CyberStat sessions with several of the 24 major federal agencies. According to DHS officials, the current approach focuses on providing CyberStat reviews for the lowest-performing agencies. However, expanding the reviews to include all 24 agencies could lead to an improved security posture.

- **Enhance FISMA reporting metrics.** In September 2013, we reported that the metrics issued by DHS for gauging the implementation of priority security goals and other important controls did not address key security activities and did not always include performance targets.[50] We recommended that OMB and DHS collaborate to develop improved metrics, and the agencies stated that they plan to implement the recommendation by September 2014.

- **Develop a strategic implementation plan.** DHS's Office of Inspector General reported in June 2013 that the department had not developed a strategic implementation plan describing its cybersecurity responsibilities and a clear plan of action for fulfilling them. According to DHS officials, it has developed this plan and is awaiting closure of the inspector general recommendation. We will review the status of this plan as part of our ongoing review of this high risk area.

- **Continue to develop continuous diagnostics and mitigation capabilities and assist agencies in developing and acquiring them.** This effort is intended to protect networks and enhance an agency's ability to see and counteract day-to-day cyber threats.

The successful implementation of these actions should result in outcomes such as enhanced DHS oversight and assistance through CyberStat, improved metrics and other outcomes, improved situational awareness,

[49] We provided DHS detail on the actions that need to be taken and outcomes that need to be achieved to address the federal information security and cyber critical infrastructure protection high-risk area. The information we provided DHS was based on our full body of work in this area.

[50] GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, GAO-13-776 (Washington, D.C.: Sept. 26, 2013).

and enhanced capabilities for assisting agencies in responding to cyber incidents. In conjunction with needed actions by federal agencies, this could contribute to improved information security government-wide.

Protecting Cyber Critical Infrastructure

DHS, in conjunction with other executive branch entities, has taken steps to enhance the protection of cyber critical infrastructure. For example, according to DHS, it has

- expanded the capacity of its National Cybersecurity and Communications Integration Center to facilitate coordination and information sharing among federal and private sector stakeholders;
- established the Information Sharing Working Group and a mechanism for creating cyber threat reports that can be shared with private sector partners; and
- set up a voluntary program to encourage critical infrastructure owners and operators to use the cybersecurity framework developed by the National Institute of Standards and Technology, as required by Executive Order 13636.

In February 2014, we identified and communicated to DHS actions critical to addressing cyber critical infrastructure protection, including the following:

- expand the Enhanced Cybersecurity Services program, which is intended to provide classified cyber threat and technical information to eligible critical infrastructure entities, to all critical infrastructure sectors as required by Executive Order 13636;
- enhance coordination efforts with private sector entities to facilitate improvements to the cybersecurity of critical infrastructure; and
- identify a set of incentives designed to promote implementation of the NIST cybersecurity framework.

Completing these efforts could assist in achieving a flow of timely and actionable cybersecurity threat and incident information among federal stakeholders and critical infrastructure entities, adoption of the cybersecurity framework by infrastructure owners and operators, and effective implementation of security controls over a significant portion of critical cyber assets. As we reported in March 2014, more needs to be done to accelerate the progress made in bolstering the cybersecurity posture of the nation and federal government. The administration and executive branch agencies need to implement the hundreds of recommendations made by GAO and agency inspectors general to address cyber challenges, resolve known deficiencies, and fully implement effective information security programs. Until then, a broad array of federal assets and operations will remain at risk of fraud, misuse, and disruption, and the nation's most critical federal and private sector infrastructure systems will remain at increased risk of attack from our adversaries.[51]

Enhancing the Sharing of Terrorism-Related Information

DHS has made significant progress in enhancing the sharing of information on terrorist threats and in supporting government-wide efforts to improve such sharing.[52] Our work on assessing the high-risk area on sharing terrorism-related information has primarily focused on federal efforts to implement the Information Sharing Environment, as called for in the Intelligence Reform and Terrorism Prevention Act of 2004.[53] The Information Sharing Environment is a government-wide effort to improve the sharing of terrorism-related information across federal agencies and with state, local, territorial, tribal, private sector, and foreign partners. When assessing progress, we review the activities of both the Program Manager for the Information Sharing Environment—a position established under the 2004 Act with responsibility for information sharing across the government—as well as efforts of DHS and other key entities, including the Departments of Justice, State, and Defense, and the Office of the Director of National Intelligence.[54] Accordingly, DHS itself is not on the high-risk list nor can DHS's efforts fully resolve the high risk issue. Nevertheless, DHS plays a critical role in government-wide sharing given its homeland security missions and responsibilities.

Overall, the federal government has made progress in addressing the terrorism-related information-sharing high-risk area. As we reported in our February 2013 update, the federal government is committed to

[51] GAO, *Government Efficiency and Effectiveness: Views on the Progress and Plans for Addressing Government-wide Management Challenges*, GAO-14-436T (Washington, D.C.: March, 12, 2014).

[52] Terrorism-related information includes homeland security, terrorism, and weapons of mass destruction information. See 6 U.S.C. §§ 482(f)(1), 485(a)(1), (5)-(6).

[53] See Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70 (2004) (codified as amended at 6 U.S.C. § 485).

[54] The Office of the Director of National Intelligence was established in 2004 to manage the efforts of the Intelligence Community. See 50 U.S.C. § 3023. Its mission is to lead intelligence integration and forge an Intelligence Community that delivers the most insightful intelligence possible.

establishing effective mechanisms for managing and sharing terrorism-related information, and has developed a national strategy, implementation plans, and methods to assess progress and results. While progress has been made, the government needs to take additional action to mitigate the potential risks from gaps in sharing information, such as ensuring that it is leveraging individual agency initiatives to benefit all partners and continuing work to develop metrics that measure the homeland security results achieved from improved sharing. We are currently conducting work with the Program Manager and key entities to determine their progress in meeting the criteria since the 2013 high-risk report.

DHS's Role in the Sharing of Terrorism-Related Information

Separately, in response to requests from this committee and other congressional committees, we have assessed or are currently assessing DHS's specific efforts to enhance the sharing of terrorism-related information. As discussed below, this work includes DHS efforts to (1) support state and major urban area fusion centers,[55] (2) coordinate with other federal agencies that support task forces and other centers in the field that share information on threats as part of their activities, (3) achieve its own information-sharing mission, and (4) share information related to the department's intelligence analysis efforts.

Fusion centers. A major focus of the high-risk area and Information Sharing Environment has been to improve the sharing of terrorism-related information among the federal government and state and local security partners, which is done in part through state and major urban area fusion centers. DHS is the federal lead for supporting these centers and has made significant strides. For example, DHS has deployed personnel to centers to serve as liaisons to the department and help centers develop capabilities (such as the ability to analyze and disseminate information), provided grant funding to support center activities, provided access to networks disseminating classified and unclassified information, and helped centers identify and share reports on terrorism-related suspicious activities. DHS has been very responsive to a recommendation in our 2010 report that calls for establishing metrics to determine what return the

[55] In general, fusion centers are collaborative efforts of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. See 6 U.S.C. § 124h(j)(1). There are 78 fusion centers in the United States.

federal government is getting for its investments in centers.[56] We have an ongoing review of DHS's efforts to assess center capabilities, manage federal grant funding, and determine the contributions centers make to enhance homeland security, and expect to issue a report later this year.

Field-based entities that share information. DHS is also taking steps to measure the extent to which fusion centers are coordinating and sharing information with other field-based task forces and centers—such as Federal Bureau of Investigation Joint Terrorism Task Forces—and assess opportunities to improve coordination.[57] In April 2013, we reported that fusion centers and other field-based entities had overlapping activities, but the agencies that support them had not held the entities accountable for coordinating and collaborating or assessed opportunities to enhance coordination, and recommended that the agencies develop mechanisms to do so.[58] In response, DHS began tracking collaboration mechanisms, such as which fusion centers have representatives from the other entities on their executive boards, are colocated with other entities, and issue products jointly developed with other entities.

DHS's efforts can help avoid unnecessary overlap in activities, which in turn can help entities leverage scarce resources. To fully address our recommendation, however, the other federal agencies must take steps to better hold their respective field entities accountable for such collaboration. In addition, these agencies must work with DHS to collectively assess nationwide any opportunities for field entities to further implement collaboration mechanisms.

DHS information-sharing mission. In September 2012, we reported that DHS had made progress in achieving its own information-sharing

[56] 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.: Sep. 29, 2010).

[57] The five types of entities we reviewed are state and major urban area fusion centers, Joint Terrorism Task Forces, Field Intelligence Groups, Regional Information Sharing Systems centers, and High Intensity Drug Trafficking Area Investigative Support Centers. DHS, the Department of Justice, and the Office of National Drug Control Policy oversee or otherwise support these entities.

[58] GAO, *Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*, GAO-13-471 (Washington, D.C.: Apr. 12, 2013).

mission, but could take additional steps to improve its efforts.[59] Specifically, DHS had demonstrated leadership commitment by establishing a governance board to serve as the decision-making body for DHS information-sharing issues. The board has enhanced collaboration among DHS components and identified a list of key information-sharing initiatives to pursue, among other things. We found, however, that five of DHS's top eight priority initiatives faced funding shortfalls. We also reported that DHS had taken steps to track its information-sharing efforts, but had not fully assessed how such efforts had improved sharing. We recommended that DHS (1) revise its policies and guidance to include processes for identifying information-sharing gaps; analyzing root causes of those gaps, and identifying, assessing, and mitigating risks of removing incomplete initiatives from its list, and (2) better track and assess the progress of key initiatives and the department's overall progress in achieving its information-sharing vision. DHS has since taken actions—such as issuing revised guidance and developing new performance measures—to address all of these recommendations.

Sharing intelligence analysis. We are finalizing a report on DHS's intelligence analysis capabilities, which are a key part of the department's efforts in securing the nation. Within DHS, the Office of Intelligence and Analysis has a lead role for intelligence analysis, but other operational components—such as CBP and ICE—also perform their own analysis activities and are part of the DHS Intelligence Enterprise. Our report, expected to be issued later this month, will address (1) the extent to which the intelligence analysis activities of the enterprise are integrated to support departmental strategic intelligence priorities, and are unnecessarily overlapping or duplicative; (2) the extent to which Office of Intelligence and Analysis customers report that they find products and other analytic services to be useful, and what steps, if any, the office has taken to address any concerns customers report; and (3) challenges the Office of Intelligence and Analysis has faced in maintaining a skilled analytic workforce and steps it has taken to address these challenges.

[59] GAO, *Information Sharing: DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts*, GAO-12-809 (Washington, D.C.: Sept. 18, 2012).

We are planning to make recommendations to help DHS enhance its intelligence analysis capabilities and related sharing of this information.[60]

Overall, DHS's continued progress in enhancing the sharing of terrorism-related information and responding to our findings and recommendations will be critical to supporting government-wide sharing and related efforts to secure the homeland.

Chairman McCaul, Ranking Member Thompson, and members of the committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contacts

For questions about this statement, please contact George A. Scott at (202) 512-8777 or scottg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

[60] The Office of Intelligence and Analysis' five customer groups are (1) DHS leadership; (2) DHS operational components; (3) Intelligence Community members; (4) state, local, tribal, and territorial partners; and (5) private critical infrastructure sectors.

(441222)

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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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.