May 7, 2014

DEPARTMENT OF HOMELAND SECURITY

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

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.

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.