December 2, 2009

# HOMELAND SECURITY

## DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-106, Statement Before the Committee on Commerce, Science and Transportation, U.S. Senate

### Why GAO Did This Study

Securing the nation's transportation and information systems is a primary responsibility of the Department of Homeland Security (DHS). Within DHS, the Transportation Security Administration (TSA) is responsible for securing all transportation modes; U.S. Customs and Border Protection (CBP) is responsible for cargo container security; the U.S. Coast Guard is responsible for protecting the maritime environment; and the National Protection and Programs Directorate is responsible for the cybersecurity of critical infrastructure. This statement focuses on the progress and challenges DHS faces in key areas of maritime, aviation, and cybersecurity. It is based on GAO products issued from June 2004 through November 2009, as well as ongoing work on air cargo security. GAO reviewed relevant documents; interviewed cognizant agency officials; and observed operations at 12 airports, chosen by size and other factors. The results are not generalizable to all airports.

### What GAO Recommends

GAO is not making recommendations in this statement; however, GAO has made prior recommendations to DHS to, among other things, analyze the feasibility of scanning U.S.-bound cargo containers and more fully protect computer-reliant critical infrastructures. DHS generally agreed with these recommendations. DHS provided technical comments on this statement, which GAO incorporated as appropriate.

View GAO-10-106T or key components.

For more information, contact Cathleen Berrick at (202) 512-8777 or berrickc@gao.gov.

### What GAO Found

DHS has made progress in enhancing security in the maritime sector, but key challenges remain. For example, as part of a statutory requirement to scan 100 percent of U.S.-bound container cargo by July 2012, CBP has implemented the Secure Freight Initiative at select foreign ports. However, CBP does not have a plan for fully implementing the 100 percent scanning requirement by July 2012 because it questions the feasibility, although it has not performed a feasibility analysis of the requirement. Rather, CBP has planned two new initiatives to further strengthen the security of container cargo, but these initiatives will not achieve 100 percent scanning. Further, TSA, the Coast Guard, and the maritime industry took a number of steps to enroll over 93 percent of the estimated 1.2 million users in the Transportation Worker Identification Credential (TWIC) program (designed to help control access to maritime vessels and facilities) by the April 15, 2009 compliance deadline, but they experienced challenges resulting in delays and in ensuring the successful execution of the TWIC pilot. While DHS and the Coast Guard have developed a strategy and programs to reduce the risks posed by small vessels, they face ongoing resource and technology challenges in tracking small vessels and preventing attacks by such vessels.

In the aviation sector, TSA has made progress in meeting the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010 and in taking steps to strengthen airport security, but TSA continues to face challenges. TSA's efforts include developing a system to allow screening responsibilities to be shared across the domestic air cargo supply chain, among other steps. Despite these efforts, TSA and the industry face a number of challenges including the voluntary nature of the program, and ensuring that approved technologies are effective with air cargo. TSA also does not expect to meet the mandated 100 percent screening deadline as it applies to air cargo transported into the U.S., in part due to existing screening exemptions for this type of cargo and challenges in harmonizing security standards with other nations. GAO is reviewing these issues as part of its ongoing work and will issue a final report next year. In addition, TSA has taken a variety of actions to strengthen airport security by, among other things, implementing a worker screening program; however, TSA still faces challenges in this area.

DHS has made progress in strengthening cybersecurity, such as addressing some lessons learned from a cyber attack exercise, but further actions are warranted. Since 2005, GAO has reported that DHS has not fully satisfied its key responsibilities for protecting the nation's computer-reliant critical infrastructures and has made related recommendations to DHS, such as bolstering cyber analysis and warning capabilities and strengthening its capabilities to recover from Internet disruptions. DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but it has not fully implemented GAO's recommendations and, thus, more action is needed to address the risk to critical cybersecurity infrastructure.