BORDER SECURITY

Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use

Why GAO Did This Study

Travel documents are often used fraudulently in attempts to enter the United States. The integrity of U.S. passports and visas depends on the combination of well-designed security features and solid issuance and inspection processes. GAO was asked to examine (1) the features of U.S. passports and visas and how information on the features is shared; (2) the integrity of the issuance process for these documents; and (3) how these documents are inspected at U.S. ports of entry. We reviewed documents such as studies, alerts, and training materials. We met with officials from the Departments of State, Homeland Security, and Commerce's National Institute of Standards and Technology, and U.S. Government Printing Office, and with officials at seven passport offices, nine U.S. ports of entry, two U.S. consulates in Mexico, and two Border Crossing Card production facilities.

What GAO Recommends

GAO recommends that State and DHS better plan for new generations of passports and visas, address potential vulnerabilities in the acceptance process of U.S. passport applications, utilize the electronic features of the new e-passport, better use the biometric feature of BCCs, and provide inspectors with systematic training prior to the issuance of new travel documents. State and DHS agreed with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1006.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jess T. Ford at (202) 512-4268 or fordj@gao.gov.
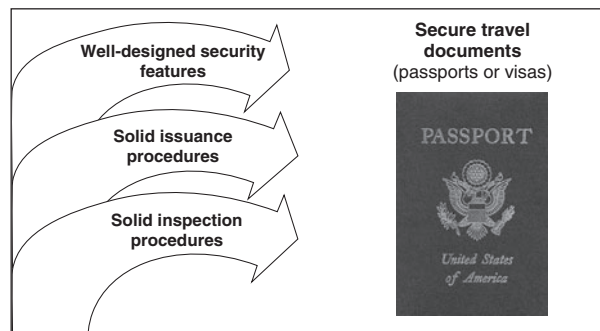
What GAO Found

The Department of State (State) has developed passports and visas, including border crossing cards (BCC), that are more secure than older versions of these documents; however, older versions have been fraudulently used and remain more vulnerable to fraud during their lifespan. For example, earlier versions valid until 2011, of which there are more than 20 million in circulation, remain vulnerable to fraudulent alteration by such means as photo substitution. Although State has updated or changed the security features of its travel documents, State does not have a structured process to periodically reassess the effectiveness of the security features in its documents against evolving threats and to actively plan for new generations.

State has taken a number of measures to ensure the security and quality of passports and visas, including establishing internal control standards and quality assurance measures, training of acceptance agents, and initiating new visa policies and procedures. However, additional measures are needed in the passport issuance process to minimize the risk of fraud. State lacks a program for oversight of the thousands of passport acceptance facilities that serve an important function in verifying the identity of millions of passport applicants each year.

Officers in primary inspection—the first and most critical opportunity to identify fraudulent travel documents at U.S. ports of entry—are unable to take full advantage of the security features in passports and visas. These officers rely on both their observations of travelers and visual and manual examination of documents to detect fraudulent documents. However, the Department of Homeland Security (DHS) has not yet provided most ports of entry with the technology tools to read the new electronic passports and does not have a process in place for primary inspectors to utilize fingerprints collected for visas, including BCCs, at all land ports of entry. Moreover, DHS has provided little regular training to update its officers on the security features and fraud trends in passports and visas.

Key Elements of a Secure Travel Document

Source: State Department (passport photo).