BORDER SECURITY

State Could Enhance Visa Fraud Prevention by Strategically Using Resources and Training

Why GAO Did This Study

Foreign nationals may apply for entry into the United States under dozens of different visa categories, depending on circumstances. State’s Bureaus of Consular Affairs and Diplomatic Security share responsibility for the prevention of visa fraud, which is a serious problem that threatens the integrity of the process. Some applicants commit fraud to obtain travel documents through illegal means, such as using counterfeit identity documents or making false claims to an adjudicating officer. Visa fraud may facilitate illegal activities in the United States, including crimes of violence, human trafficking, and terrorism. This report examines (1) countries and visa categories that are subject to the most fraud; (2) State’s use of technologies and resources to combat fraud; and (3) training requirements of State officials responsible for fraud prevention. GAO examined State’s reports and data on fraud trends and statistics, examined resources and technologies to counter fraud, and observed visa operations and fraud prevention efforts overseas and domestically.

What GAO Found

Certain countries and visa categories are subject to higher levels of fraud. In fiscal year 2010, almost 60 percent of confirmed fraud cases (9,200 out of 16,000) involved applicants from Brazil, China, Dominican Republic, India, and Mexico. Department of State (State) officials told GAO that fraud most commonly involves applicants for temporary visits to the United States who submit false documentation to overcome the presumption that they intend to illegally immigrate. Fraud is also perpetrated for immigrant visas and nonimmigrant visa categories such as temporary worker visas and student visas. In response to State efforts to combat visa fraud, unscrupulous visa applicants adapt their strategies, and as a result, fraud trends evolve over time.

State has a variety of technological tools and resources to assist consular officers in combating fraud, but does not have a policy for their systematic use. For example, State recently implemented fraud prevention technologies such as a fraud case management system that establishes connections among multiple visa applications, calling attention to potentially fraudulent activity. Overseas posts have Fraud Prevention Units that consist of a Fraud Prevention Manager (FPM) and locally employed staff who analyze individual fraud cases. In 2011, the ratio of Fraud Prevention Unit staff to fraud cases varied widely across overseas posts, causing disproportionate workloads. The Kentucky Consular Center (KCC) is a domestic resource available to posts that verifies information on certain visa applications. However, KCC services are only provided on an ad-hoc basis, and State does not have a policy for posts to systematically utilize its resources. For example, an FPM at a high fraud post told GAO that the post would like to utilize KCC anti-fraud services for screening certain visa categories, but did not know how to request KCC assistance.

Although State offers anti-fraud training courses at the Foreign Service Institute and online, it does not require FPMs to take them and does not track FPMs’ enrollment. Consular officers receive limited fraud training as part of the initial consular course, and FPMs are not required to take advanced fraud training in new technologies. In addition, GAO found that 81 percent of FPM positions were filled by entry-level officers and 84 percent of FPM positions were designated as either part-time or rotational. Between October 2009 and July 2012, entry-level officers made up about 21 percent of the total students who registered for a course on detecting fraudulent documents, and State could not guarantee that FPMs were among them. Four out of the five FPMs with whom GAO spoke had not been trained in State’s new fraud case management system.

What GAO Recommends

GAO recommends that State (1) formulate a policy to systematically utilize anti-fraud resources available at KCC, based on post workload and fraud trends, as determined by the Department and (2) establish requirements for FPM training in advanced anti-fraud technologies, taking advantage of distance learning technologies, and establishing methods to track the extent to which requirements are met. State concurred with these recommendations.

View GAO-12-888. For more information, contact Michael Courts at (202) 512-8980 or courtsm@gao.gov.