United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2012

BORDER SECURITY

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

GAO-12-888

September 2012

BORDER SECURITY

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

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-888, a report to congressional requesters

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 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.

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.

Visa Applicants at a High Fraud Post Wait for Interviews with Consular Officials

Source: State.

Contents

Figures

Abbreviations

ARSO-I	Assistant Regional Security Officer - Investigator
DHS	U.S. Department of Homeland Security
ECAS	Enterprise Case Assessment Service
ICE	Immigration and Customs Enforcement
KCC	Kentucky Consular Center
LES	Locally Employed Staff
MATRIX	Match Analytics and Trusted Real-time Identity X-Ref (or cross-reference)
MLB	Major League Baseball
RSO	Regional Security Officer
State	U.S. Department of State
SWT	Summer Work Travel
USCIS	U.S. Citizenship and Immigration Services

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 10, 2012

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Department of State's (State) visa issuance process is the first line of defense against fraudulent or unlawful entry into the United States. State issues visas for both temporary visitors (referred to as nonimmigrant visas) and those seeking to enter the United States as permanent immigrants (referred to as immigrant visas). There are dozens of visa categories for entry, such as tourist visas, student visas, and temporary worker visas (see app. II for a list of all temporary visitor visa categories). State seeks to identify and prevent attempts by applicants to obtain travel documents through unauthorized means, such as knowingly altering or using counterfeit identity documents or intentionally making false claims or statements. Some applicants use fraudulently obtained visas to facilitate illegal activities in the United States, including crimes of violence, narcotics, human trafficking, and terrorism.

In 2005, we reported that State and other agencies had taken many steps to strengthen the visa process as an antiterrorism tool since the September 11, 2001 attacks. For example, State increased hiring of consular officers, revamped consular training with a focus on counterterrorism, and increased resources to combat visa fraud.[1] In 2007, we reported that the security of visas had been enhanced but more needed to be done to prevent their fraudulent use.[2] That same year, we

[1]GAO, *Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, GAO-05-859 (Washington, D.C.: Sept.13, 2005).

[2]GAO, *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use*, GAO-07-1006 (Washington, D.C.: July 31, 2007).

reported that the Diversity Visa Program is particularly vulnerable to manipulation from an unscrupulous visa industry in some countries.[3]

This report examines (1) countries and visa categories subject to the most visa fraud; (2) State's technologies and resources to combat fraud; and (3) training requirements of State officials responsible for fraud prevention.

To determine the countries and visa categories subject to the most visa fraud, we analyzed State Fraud Digest reports from 1996 through 2012, reviewed fraud summaries for posts with high rates of fraud, reviewed compilations of Diplomatic Security Monthly Status reports, analyzed data on the number of visa applications referred to Fraud Prevention Units, and interviewed State officials at headquarters and abroad to discuss fraud trends. To assess State's use of technologies and resources to combat fraud, we met with State's Bureau of Consular Affairs Office of Consular Systems and Technology to review State's major data systems as well as the latest technological tools available to consular officers and Fraud Prevention Managers, and we visited the Kentucky Consular Center (KCC) to observe prescreening and anti-fraud activities. To understand the training required of State officials responsible for combating fraud, we gathered information about the training requirements of Fraud Prevention Managers and staff working in Fraud Prevention Units. We also analyzed data on the experience level of Fraud Prevention Managers at all 222 visa-issuing posts. Lastly, we conducted interviews with consular officials and Diplomatic Security Special Agents working in five overseas posts on issues related to visa fraud prevention.

We conducted our work from August 2011 through September 2012, 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

[3]GAO, *Border Security: Fraud Risks Complicate State's Ability to Manage Diversity Visa Program*, GAO-07-1174 (Washington, D.C.: Sept. 21, 2007). The program provides up to 55,000 immigrant visas each fiscal year to aliens from countries with low rates of immigration to the United States. Diversity visas provide an immigration opportunity to individuals from such countries.

conclusions based on our audit objectives. (see appendix I for more information about our scope and methodology).

Background

The mission of State's Bureau of Consular Affairs (Consular Affairs) is to protect the lives and interests of U.S. citizens overseas and to strengthen U.S. border security through the vigilant adjudication of U.S. passports and visas. Consular officers abroad have sole legal authority to adjudicate visa applications, and they receive overseas and domestic support to help identify visa fraud. Consular officers at overseas posts issue nonimmigrant visas to temporary visitors and immigrant visas to people who intend to immigrate to the United States.[4] The adjudication processes for both nonimmigrant and immigrant visa applications contain steps to check for fraud.

Consular Officers Rely on Overseas Support to Identify Fraud

Consular Affairs has more than 11,000 officers, local staff, and contractors working in over 300 locations around the world, including domestic visa centers and passport facilities. Within each consular section at overseas posts, consular officers adjudicate visa applications, serving as fraud detection officers on the first line of defense for border security. Consular officers are charged with facilitating legitimate travel while preventing ineligible aliens, including potential terrorists, from gaining admission to the United States. To help detect and prevent fraud, consular officers work with members of a Fraud Prevention Unit located in the consular section. In large posts, the Fraud Prevention Unit may be led by a Fraud Prevention Manager, and may be augmented at certain high-fraud posts by a Diplomatic Security Assistant Regional Security Officer Investigator.[5] In smaller posts, the Fraud Prevention Manager may be a consular officer who has other responsibilities depending on the workload volume and prevalence of fraud at the post. Consular officers may also coordinate with a Department of Homeland Security (DHS) Visa Security Officer and an external anti-fraud working group.

[4]The issuance of all visas is governed by the Immigration and Nationality Act of 1952 as amended by subsequent immigration legislation.

[5]See appendix III for specific case studies of the Fraud Prevention Unit and the Assistant Regional Security Officer Investigator.

- *Fraud Prevention Manager*. Under the Bureau of Consular Affairs, fraud prevention efforts at the 222 visa-issuing posts are led by a Fraud Prevention Manager—a Foreign Service Officer assigned by consular management to investigate fraud cases, conduct fraud training, and provide information on fraud trends to the entire consular section. As of April 30, 2012, 81 percent of all visa issuing posts (180 of 222) had Fraud Prevention Manager positions filled by an entry-level officer or an officer of unspecified grade, and 84 percent of visa issuing posts (186 of 222) had Fraud Prevention Manager positions designated as part- time or rotational.[6] As of April 30, 2012, 36 posts had full-time mid-level Fraud Prevention Managers serving for 2 years. An additional 40 posts had full-time entry-level Fraud Prevention Managers serving for 2 years in positions originally designated for mid-level officers. Officers assigned to part-time Fraud Prevention Manager positions have other consular-related duties in addition to preventing fraud. An officer filling the position on a rotational basis serves as the Fraud Prevention Manager for a designated period of time, typically 6 months, before moving on to other duties. State officials told us that the reason most Fraud Prevention Manager positions are part-time or rotational is in order to provide consular managers more flexibility in how they use consular staff, and also to provide officers with more opportunities to work on different activities.

- *Fraud Prevention Unit*. At 94 percent of visa-issuing posts (208 of 222), Fraud Prevention Managers have locally employed staff to assist them in fraud investigations, forming a Fraud Prevention Unit.[7] Out of the 3,700 locally employed staff working at consular posts, 417 are assigned to Fraud Prevention Units. These staff generally have special expertise in host country culture and language, as well as a network of local contacts to help develop leads on possible fraud. The Fraud Prevention Unit collects and verifies data for use in identifying fraud trends, analyzes individual fraud cases, and drafts and disseminates fraud reports. Tools utilized in individual fraud investigations vary from post to post, but may include physical

[6]For more information on State staffing, see GAO, Department of State: *Foreign Service Midlevel Staffing Gaps Persist Despite Significant Increases in Hiring,* GAO-12-721 (Washington, D.C.: June 14, 2012).

[7]Not all consular posts have a dedicated Fraud Prevention Unit. Some posts are very small and provide limited consular services (such as only American Citizen Services, and no visa services).

document examination, visa record searches, facial-recognition review, phone calls to verify data, Internet searches, and site visits. Once all of the data have been collected, verified, and assessed, the Fraud Prevention Manager reviews the results and provides a final fraud finding to consular officers, who use the information to make a determination on whether to issue a visa to the applicant. If the Fraud Prevention Manager determines that the visa fraud may involve criminal activity, the case may be referred to Diplomatic Security agents at post for further investigation.

- Assistant Regional Security Officer Investigator. Under the Bureau of Diplomatic Security, 84 Assistant Regional Security Officer Investigators (ARSO-I) are assigned to 75 high-fraud posts to protect the integrity of the visa system and disrupt criminal networks and terrorist mobility.[8] ARSO-Is are Diplomatic Security Special Agents who specialize in criminal investigations of visa fraud.[9] Diplomatic Security recommends that ARSO-Is spend 80 percent of their time working on visa fraud, and 20 percent of their time supporting other Diplomatic Security responsibilities, such as providing security to high-level visitors at post. ARSO-Is often work with local law enforcement and judicial officials to arrest and prosecute violators of local laws related to visa fraud, such as the fraudulent production of local identification documents used in applications for visas. Some investigations are connected to large-scale alien smuggling or human trafficking cases.

- DHS's U.S. Immigration and Customs Enforcement (ICE) Visa Security Program. ICE deploys Visa Security Officers to assist the consular section at designated high-risk posts by providing advice and training to consular officers regarding specific security threats, reviewing visa applications, and conducting investigations with

[8]By the summer of 2013, Diplomatic Security plans to have 105 ARSO-Is working in 93 posts in 63 countries, according to Diplomatic Security officials.

[9]Diplomatic Security assigns ARSO-Is based on a number of factors including the number of visas adjudicated and visa refusal rates. At posts without an ARSO-I, the Diplomatic Security Regional Security Officer is responsible for criminal investigations of visa fraud. However, Regional Security Officers have numerous responsibilities, such as physical security of the compound, and according to State officials are not able to dedicate a large portion of their time to investigating visa fraud.

respect to consular matters under the jurisdiction of the Secretary of Homeland Security.[10]

- External Anti-Fraud Working Group. At some posts, members of the Fraud Prevention Unit may coordinate with officials from other countries' embassies and consulates to share fraud trends in an anti-fraud working group.

Consular Officers Also Rely on Domestic Fraud Prevention Efforts

Domestically, both State and DHS play a role in fraud prevention and detection. While the Secretary of State has the lead role with respect to foreign policy-related visa issues, DHS is responsible for reviewing implementation of the policy and providing additional direction.

- State's Bureau of Consular Affairs Visa Office has direct responsibility for visa policy and oversight for the operations of KCC and the National Visa Center in New Hampshire.[11] These two centers prescreen visa applications for fraud and provide other support for visa adjudication worldwide.

- State's Bureau of Consular Affairs Office of Fraud Prevention Programs advises posts on visa and passport fraud questions, develops training material to manage fraud prevention programs, produces publications on fraud issues and trends, and coordinates with other U.S. agencies involved in preventing visa fraud.

- State's Diplomatic Security Office of Overseas Criminal Investigations Branch provides managerial oversight, guidance, and support to ARSO-Is at overseas posts.

- Diplomatic Security domestic field offices support overseas investigations by investigating visa fraud that is connected to criminal networks within the United States.

[10]For more information on the Visa Security Program, see *GAO, Border Security: DHS's Visa Security Program Needs to Improve Performance Evaluation and Better Address Visa Risk Worldwide*, GAO-11-315 (Washington, D.C.: Mar. 31, 2011).

[11]KCC is a centralized nonimmigrant and diversity visa processing facility. The National Visa Center is a centralized immigrant visa processing facility.

- DHS's U.S. Citizenship and Immigration Service (USCIS), Fraud Detection National Security Directorate is responsible for detecting, pursuing, and deterring immigration benefit fraud, and identifying persons seeking benefits who pose a threat to national security and public safety. In addition, Fraud Detection National Security Directorate staff conduct site visits and administrative inquiries within the United States on persons or entities suspected of immigration fraud and follow up with ICE investigators, law enforcement, and intelligence agencies on potential national security risks identified during background checks on immigration benefit applications.

- DHS's ICE Document and Benefit Fraud Task Forces work with federal, state, and local partners to detect, deter, investigate, and present instances of benefit fraud for criminal prosecution.

- DHS's Customs and Border Protection agents serve as the last line of defense in protecting American borders. Customs and Border Protection agents verify that visitors have proper travel documents and valid visas, and have the discretion to not admit travelers with valid visas into the United States if the agent suspects the traveler intends to violate the terms of his or her visa.

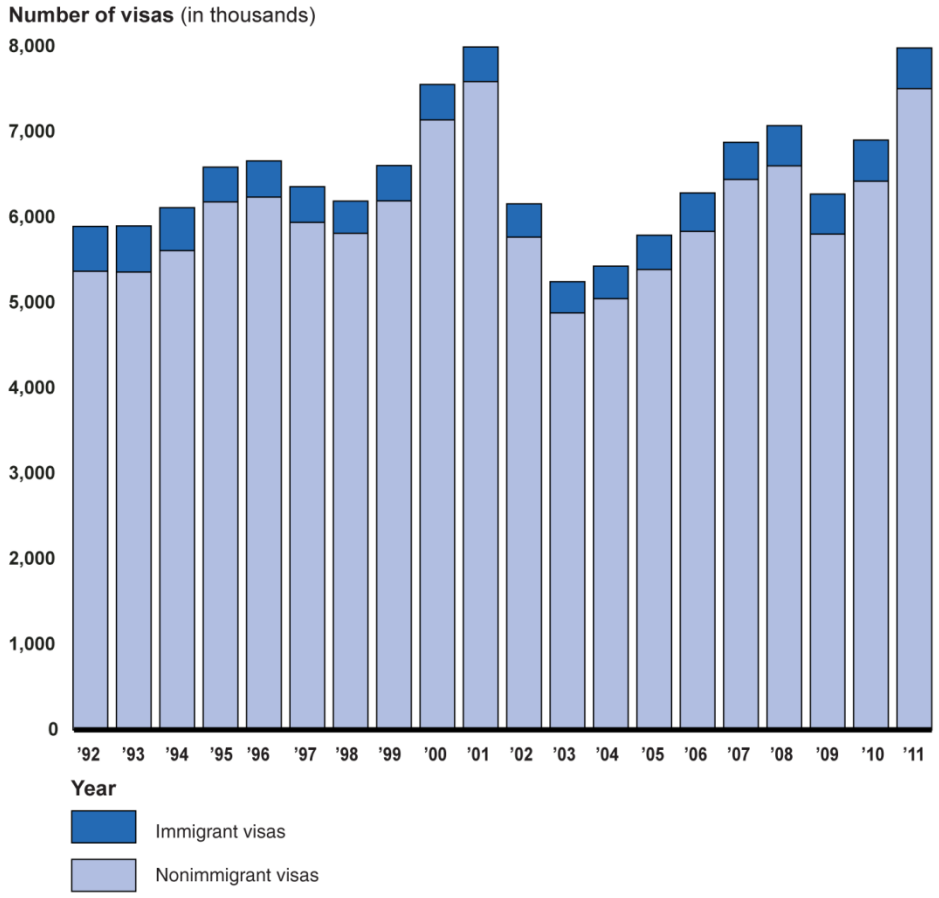
Issuance of Visas Has Generally Increased since 2003

After the September 11, 2001 terrorist attacks, the number of visas issued initially declined, but has generally increased steadily since 2003, and State anticipates demand for visas to continue to rise. As seen in figure 1, in 2001, the United States issued almost 8 million nonimmigrant and immigrant visas, based on data from the Consular Consolidated Database.[12] From 2001 to 2003, visa issuances declined by 34 percent. However, since then, the number of immigrant and nonimmigrant visas issued has generally trended upward. In 2011, consular officers issued more than 7.5 million nonimmigrant visas, up 54 percent from 2003 levels. Approximately 75 percent of the 7.5 million nonimmigrant visas issued in 2011 were processed for temporary visits to the United States for business or personal reasons, such as tourism.[13] More than half (52 percent) of the visas for temporary visits were issued to visitors from Brazil, China, India, and Mexico. According to the Deputy Assistant Secretary for Visa Services, State continues to see increases in visa demand for individuals residing in some of the world's fastest-growing economies.

[12]The Consular Consolidated Database contains passport, nonimmigrant visa, and immigrant visa application information that has been collected since 1999.

[13]These data include border crossing cards issued to Mexican nationals.

Figure 1: Nonimmigrant and Immigrant Visas Issued Worldwide, Fiscal Years 1992 to 2011



Source: GAO analysis of State data.

While visa issuances have generally increased since 2003, visa refusals have fluctuated since 2006. In fiscal year 2011, more than 2.1 million nonimmigrant visa applicants worldwide were denied visas for entry into

the United States.[14] As seen in table 1, adjusted refusal rates for tourist visas in Brazil, China, India, and Mexico fluctuated between fiscal years 2006 and 2011.[15] While refusals of visitors from Brazil, China, and Mexico have generally decreased in the last 6 years, refusals of visitors from India have increased. Visas may be refused for a number of reasons other than a suspicion of fraud, such as insufficient documentation or suspected immigration intent.[16] When a consular officer suspects that the applicant's travel or financial documents are counterfeit, the consular officer may deny the applicant's request for a visa or may refer the case to the Fraud Prevention Unit for an additional fraud assessment.[17]

[14]Approximately 775,000 of the 2.1 million refusals were waived or overcome in fiscal year 2011. The Immigration and Nationality Act contains provisions that may allow a visa applicant who was denied a visa for a particular ineligibility to apply for a waiver of that ineligibility. DHS adjudicates all waivers of immigrant and nonimmigrant visa ineligibility. Waivers are discretionary, meaning that there are no guarantees that DHS will approve a waiver. If the waiver is approved, the applicant can be issued a visa. For nonimmigrant visa waivers, the consular officer must first choose to recommend to DHS that the applicant be considered for a waiver.

[15]Visa applicants who are deemed ineligible and refused nonimmigrant visas may apply, and State may choose to overcome the initial refusal or the applicant may apply for a waiver. The information in table 1 depicts adjusted refusal rates based on both overcomes and waivers.

[16]Under section 214(b) of the Immigration and Nationality Act,[8 U.S.C. 1184(b)], an applicant for a nonimmigrant visa is generally presumed to be an intending immigrant until the applicant can demonstrate to the satisfaction of an interviewing consular officer that they are entitled to the type of visa for which they are applying and that they will depart the United States at the end of their authorized temporary stay.

[17]An applicant who, by fraud or willful misrepresentation of a material fact, attempts to obtain a visa or admission into the United States is inadmissible under section 212(a)(6)(C)(i) of the Immigration and Nationality Act.

Table 1: Percentage of Tourist Visas Refused in Brazil, China, India, and Mexico, Fiscal Years 2006 to 2011

Country	2006	2007	2008	2009	2010	2011
Brazil	13	10	6	7	5	4
China	25	21	18	16	13	12
India	20	22	25	29	27	30
Mexico	31[a]	33[a]	11[a]	11[a]	11	13

Source: GAO analysis of State data in the Consular Consolidated Database.

[a]Does not include border crossing card applications.

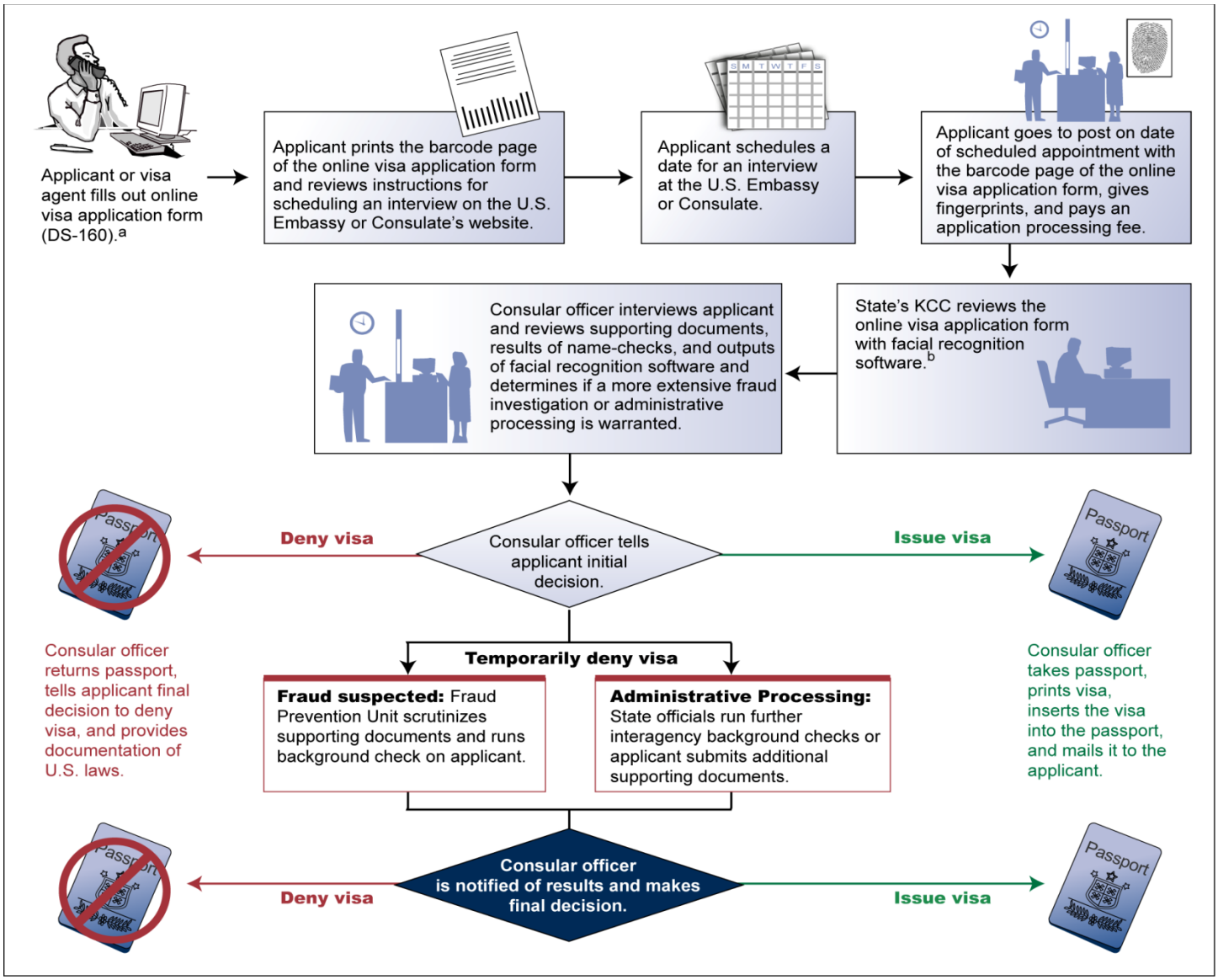
The U.S. travel and tourism industry benefits from foreign visitors, and the U.S. government is working to accommodate an increase in demand for tourist travel. For example, State reported in 2010 that international tourists contributed $134 billion to the U.S. economy and supported over 1.1 million jobs. The Administration has encouraged State to increase visa processing capacity and reduce wait times for receiving a visa. In January 2012, President Obama issued an Executive Order requesting that the Secretaries of State and Homeland Security, in consultation with the Assistant to the President for Homeland Security and Counterterrorism and the Director of the Office of Management and Budget, develop an implementation plan to (1) increase nonimmigrant visa processing capacity in China and Brazil by 40 percent over the coming year and (2) ensure that 80 percent of nonimmigrant visa applicants are interviewed within 3 weeks of receipt of visa applications.

Nonimmigrant and Immigrant Visa Adjudication Processes Include Fraud Checks

Nonimmigrant Visa Adjudication Process

Almost all nonimmigrant visa applicants submit an online visa application called the DS-160 through State's web-based portal called the Consular Electronic Application Center, and then schedule a visa interview at a local U.S. embassy or consulate. Consular officers interview visa applicants, review the application and supporting documents, such as birth certificates, and make an initial decision to issue or deny the visa application. A consular officer may temporarily deny the visa in order to scrutinize the application for suspected fraud or to process it further administratively (see fig. 2).

Figure 2: Standard Nonimmigrant Visa Adjudication Process at a U.S. Embassy or Consulate



Source: GAO analysis of State data; Nova Development (clip art).

[a]Prior to this step, some nonimmigrant visas require petitioners to file a petition on behalf of the applicant with USCIS. USCIS is responsible for approving or denying the petition, notifying the petitioner, and sending the approved petition to KCC, where a file is created in the Petition Information Management System.

[b]KCC also prescreens work visas submitted to 24 high-fraud, high-volume posts based on information provided in the USCIS petition. Relevant information is entered into the comments on the DS-160 for consular officers to review at the time of the interview.

Immigrant Visa Adjudication Process

Obtaining an immigrant visa is one part of a four part process for aliens outside of the United States to become a permanent resident of the United States. First, an eligible U.S. citizen or lawful permanent resident, called a petitioner, must file a petition (a paper form) with USCIS on behalf of the alien applying for lawful permanent resident status, who is called the beneficiary. Generally, the petitioner can be either a relative[18] or employer, although there are visa categories in which the applicant can self petition, such as the diversity visa.[19] USCIS has the sole authority to approve or deny the petition. Second, once a petition is approved and a visa number is available in the appropriate category, the beneficiary prepares for a visa interview by gathering required documentation and undergoing a medical exam. Third, the beneficiary, now called the applicant, submits an online visa application, either the DS-260 or the DS-230, along with evidence supporting the applicant's eligibility, such as a birth certificate or diploma.[20] All aliens outside the United States apply for an immigrant visa at the U.S. consulate in their current country of residence. As in the nonimmigrant visa process, the alien schedules a visa interview, submits fingerprints, and pays a visa application processing fee. During the interview, a consular officer reviews submitted documentation as well as biometric and other security and fraud checks, determines if the alien is subject to any ineligibilities, and confirms that the applicant has the required legal relationship with the petitioner. The consular officer then either approves or denies the visa application. If the visa application is approved, a visa is printed and placed in the applicant's passport. Fourth, the applicant travels to the United States with his or her immigrant visa and packet of supporting documentation. Upon admission

[18]For U.S. citizens petitioning for a family member, immediate relatives include spouses, parents of citizens ages 21 and older, and citizens' unmarried children under age 21. There is no limit on the number of immediate relatives of U.S. citizens that can seek lawful permanent residency. U.S. citizens may also petition for adult children and for siblings; and there are numerical limits on these categories. For lawful permanent residents petioning for a family member, the family member must be a spouse, a child or an unmarried adult son or daughter; and there are numerical limits.

[19]Permanent residency based on employment may be provided to aliens such as (1) professionals with advanced degrees, (2) persons with exceptional ability, (3) skilled or professional workers, (4) special immigrants, and (5) immigrant investors. Immigration law limits the annual number of employer-sponsored immigrants.

[20]The DS-260 is an online immigrant visa form that is replacing the DS-230, a paper form. State is in the process of rolling out the DS-260 around the world, according to State officials.

by a Customs and Border Patrol officer at the port of entry, the alien becomes a lawful permanent resident.

Certain Countries and Visa Categories Experience High Levels of Fraud, but Trends Evolve over Time

Certain countries, such as Brazil, China, the Dominican Republic, India, and Mexico, had high numbers of suspected fraud cases in fiscal year 2010, and certain visa categories, such as work visas, student visas, and diversity visas, had high levels of fraud. Visa fraud has become more sophisticated over time with increased globalization, advanced technology, and ease of travel.

Although Fraud Conditions Are Post-Specific, Certain Countries Have High Numbers of Suspected Fraud Cases

State requires Fraud Prevention Managers to classify fraud levels at each post. Fraud Prevention Managers are required to submit a fraud assessment twice a year as part of the post's bi-annual fraud summary. Fraud assessments rank a post's fraud conditions as high, medium, or low, based on the ratio of visa applications referred to the Fraud Prevention Unit out of the total number of visa applications. The fraud assessment also includes the prevalence of corruption in the local environment, including the reliability of country documents and cooperation with local law enforcement. Additionally, ARSO-Is provide input into fraud assessments regarding the nature of criminal activity involving visas. According to State, a country with high numbers of suspected fraud cases may not necessarily be designated as a high-fraud country if its proportion of suspected fraud to visa applications is low.

Recently, State has taken steps to improve its ability to compare fraud levels across posts. In the past, according to State officials, self-reported fraud levels had not been used to assess posts' fraud conditions relative to other posts because posts had different methods for referring cases to Fraud Prevention Units.[21] Referrals to Fraud Prevention Units are considered an accurate portrayal of the volume of fraud cases handled at individual posts because Fraud Prevention Managers must make a fraud

[21]In June 2005, State's Office of Fraud Prevention Programs developed a one-time fraud ranking of posts that included weighted criteria based on demographics, immigrant and nonimmigrant visa refusal rates, DHS statistics on adjustments of status by country, posts' own assessments of fraud, and a country corruption index. This one-time ranking was primarily used to assist in deliberations on ARSO-I placement.

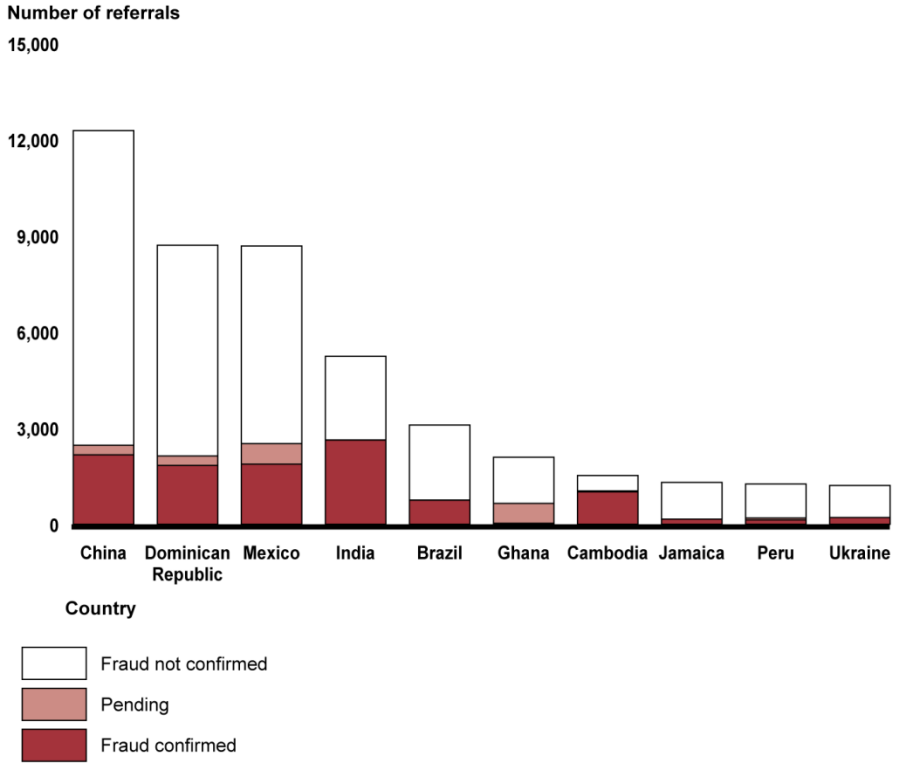
assessment for all cases that are referred. In July 2012, State distributed new guidance that clarifies when consular officers should refer visa applications to Fraud Prevention Units. For example, new guidance instructs consular officers to refer applications to Fraud Prevention Units whenever the unit is expected to expend resources to verify some aspect of an applicant's case or when consular officers cannot perform a needed task, such as verifying the employment of an applicant.

The volume of visas processed and the number of fraudulent applications vary from country to country. In general, fraudulent activity is found in a very small percentage of overall visas granted. Based on State's Consular Consolidated Database, 6.9 million nonimmigrant and immigrant visas were issued worldwide in 2010. That same year, approximately 74,000 visa applications were referred to Fraud Prevention Units for additional scrutiny. Of these, about 16,000, or 22 percent, were confirmed as fraudulent in fiscal year 2010.[22] Some countries may experience high visa demand but low numbers of suspected fraud cases, while other countries may experience high visa demand and high numbers of suspected fraud cases. For example, in 2010, consular officers throughout Brazil issued approximately 556,000 visas and referred about 3,000 visa applications to their Fraud Prevention Units, of which 750 (or 24 percent of visa applications suspected of fraud) were confirmed as fraudulent. Meanwhile, consular officers throughout India issued about 528,000 visas in 2010, referred about 5,200 visa applications to their Fraud Prevention Units, and confirmed about 2,600 (or 50 percent of visa applications suspected of fraud) as fraudulent. See figure 3 for the top 10 posts for referrals to Fraud Prevention Units among total nonimmigrant and immigrant visa applications in 2010. Almost 60 percent of confirmed fraud cases (9,200 out of 16,000) were referred to Fraud Prevention Units in Brazil, China, Dominican Republic, India, and Mexico in fiscal year 2010.[23]

[22]State's suspected and confirmed fraud case data for fiscal year 2011 were divided into two data systems, and some cases may have been double-counted. We determined that State's data for fiscal year 2010 were more reliable for our purposes.

[23]These countries have many fraud cases because they process a high volume of visas.

Figure 3: Top 10 Countries for Referrals to Fraud Prevention Units, Fiscal Year 2010



Source: GAO analysis of State data.

Visa Fraud Concentrated in Nonimmigrant Visa Applications

State's Office of Fraud Prevention Programs reports that a majority of visa fraud involves nonimmigrant visa applicants who submit false documents or make false statements to obtain a tourist or business visitor visa. According to State officials, some visitor visa applicants provide fraudulent statements or documents, such as a false bank statement, to demonstrate strong ties with their home country and therefore overcome the presumption that they intend to use their temporary visitor visa to illegally immigrate to the United States. Denied visitor visa applications are not usually referred to the Fraud Prevention Unit unless the officer suspects the case could be linked to organized crime.

Other kinds of fraud can be found in temporary worker visas, student visas, exchange visitor visas, immigrant visas, and diversity visas.

- *Temporary Worker Visas*: While State officials said that most work visas facilitate legitimate travel, fraud has been found among

petitioners and applicants for both skilled worker and temporary agricultural worker visas.[24] Some petitioners in the United States create phony companies and petition for workers to join them in the United States, usually with the applicants' knowledge and participation in the fraudulent activity, according to State officials. Other examples of fraud include cases in which educational degrees were found to be fraudulent, signatures were forged on supporting documents, and workers performed duties or received payments significantly different from those described in the applications. A recent DHS study reported that 21 percent of skilled worker petitions they examined involved fraud or technical violations.[25] In 2005, DHS began collecting an additional $500 fee on certain work visas to be used for fraud prevention and detection purposes.[26]

- *Student Visas*: Foreign students interested in studying in the United States must first be admitted to a school or university before applying for a visa at a U.S. embassy or consulate overseas.[27] The process for

[24]The most common of these types of visas are H and L visas. H visas are for temporary workers and L visas are for intracompany transfers. In 2011, 56 percent of all skilled worker visas (H-1B) were issued to citizens of India and 94 percent of all temporary agricultural visas (H-2A) were issued to citizens of Mexico. For more information, see *Visa Program: Reforms Are Needed to Minimize the Risks and Costs of Current Program*, GAO-11-26 (Washington, D.C.: Jan. 14, 2011).

[25]As a result of the findings of this study and others, USCIS launched an Administrative Site Visit and Verification Program (ASVVP) —an ongoing program to visit work sites of companies hiring skilled workers and considered to be at a higher risk for abusing the program, according to officials. All H1-B ASVVP cases are randomly selected. During fiscal year 2010, USCIS conducted 14,433 skilled worker visa site inspections, which resulted in 948 adverse actions, such as the revocation or denial of benefits, or the referral of a case for criminal investigation.

[26]H-1B Visa Reform Act of 2004, Pub. L. No. 108-447, Div. J, Title IV, Section 426, 118 Stat. 3357. In addition, legislation established an additional fee of $2,000 for petitions filed through September 30, 2015, for petitioners with 50 or more employees in the United States and more than 50 percent of those U.S. employees on H-1B or L visas. Pub. L. No. 111-230, § 402(b), 123 Stat. 2485, 2487, as amended by Publ. L. No 111-347, § 302, Jan. 2, 2011, 124 Stat. 3667.

[27]Students are granted F and M visas. F visas are for study at academic institutions and M visas are for study at vocational or nonacademic institutions. According to State's regulations, a student visa applicant must meet the following requirements to qualify: (1) acceptance at an approved school; (2) possession of sufficient funds; (3) sufficient knowledge of the English language to undertake the chosen course of study or training (unless coming to participate exclusively in an English language training program); and (4) present intent to leave the United States at conclusion of studies. See 22 C.F.R. § 41.61(b)(1) and 8 U.S.C. § 1101(a)(15)(F) and § 1101(a)(15)(M).

determining who will be issued or refused a visa contains several steps, including documentation reviews, in-person interviews, collection of applicants' fingerprints, and cross-references against multiple databases of information.[28] In 2011, State issued over 486,000 student visas, of which 71 percent were issued to students from Asia. According to the Fraud Prevention Coordinator for India, fraud among student visa applications is common throughout India. For example, some exam centers that offer the Test of English as a Foreign Language (TOEFL) are suspected of being complacent when students cheat on the exam in order to achieve high scores. If a student applicant cannot answer a consular officer's questions in English, yet received 105 out of 120 on their TOEFL score, fraud may be present, according to a consular officer in New Delhi.

- *Exchange Visitor Visas*: Summer Work and Travel (SWT) visas are a subset of the Exchange Visitor Program, and are susceptible to fraud.[29] The Exchange Visitor Program fosters global understanding through educational and cultural exchanges. All exchange visitors are expected to return to their home country upon completion of their program in order to share their experiences. In 2011, 35 percent (108,717) of the total exchange visitors (306,429) were granted entry into the United States for the purpose of "Summer Work and Travel." According to State officials, many SWT visa applicants misrepresent their status as students or their intentions for using the SWT visa. Additionally, many U.S. sponsors falsely represent their businesses and how they intend to employ SWT applicants. U.S. sponsors have been found to exploit SWT visa holders for financial gain. On May 10, 2012, State's Bureau of Education and Cultural Exchange issued rules that are expected to protect the health, safety, and welfare of SWT program participants. The rules provide a cap on the number of annual SWT program participants that may be granted visas.[30]

[28]For more information, see GAO, *Student and Exchange Visitor Program, DHS Needs to Assess Risks and Strengthen Oversight Functions,* GAO-12-572 (Washington, D.C.: June 18, 2012).

[29]Exchange visitors are granted J visas. J visas do not involve petitioners, and are therefore not screened in the same manner as petition-based applications, according to State officials.

[30]See 77 Fed. Reg. 27593 to be codified at 22 C.F.R. PART 62.

- *Immigrant Visas*: In 2010, State issued 482,052 immigrant visas. That same year, 21,013 immigrant visa applications were referred to Fraud Prevention Units and 4,984 (or about 24 percent) were confirmed as fraudulent. Immigrant visa fraud can take many forms. At several posts we visited, State officials said a common problem involved applicants who pay American citizens to marry them or who falsely represent their intentions to citizens and deceive them into marriage in order to obtain lawful permanent residence in the United States. In a typical immigrant visa fraud case, an individual divorces his or her spouse in a foreign country, marries an American citizen, and, after living in the United States for a certain period of time, obtains U.S. citizenship or legal permanent resident status, divorces the U.S. spouse, and remarries the original spouse so that they can reunite in the United States.

- *Diversity Visas*: The Diversity Visa Program was established through the Immigration Act of 1990 and provides up to 55,000 immigrant visas annually to aliens from countries with low rates of immigration to the United States.[31] Aliens register for the diversity visa lottery for free online and applicants are randomly selected for interviews through a lottery process. Upon being selected, a winner must apply for a visa, be interviewed, and be found eligible for the diversity visa. All countries are eligible for the Diversity Visa Program except those from which more than 50,000 immigrants have come to the United States over the preceding 5 years. In 2011, approximately 16.5 million people applied for the program and about 107,000 (7 percent) were selected for further processing. Of those selected, 75,000 were interviewed at posts for a diversity visa, and approximately 50,000 received visas. Because the program does not require a U.S.-based petitioner, it is particularly susceptible to fraud. Diversity visa fraud is rampant in parts of South Asia, Africa, and Eastern Europe, and is particularly acute in areas where few individuals have independent access to the Internet.[32] A typical scenario includes visa facilitators, travel agents, or Internet café operators who help would-be applicants submit an entry for a fee. Many of these facilitators withhold the confirmation information that the entrant must use to retrieve his or

[31]Immigration Act of 1990, Pub. L. No. 101-649, § 131, 104 Stat. 4978, 4997-99 (1990) (codified at 8 U.S.C. § 1153 (c).

[32]In fiscal year 2011, between 5,000 and 6,000 individuals were registered for diversity visas from Bangladesh, Ethiopia, Ghana, Nigeria, and Ukraine.

her selection status. To access the lottery notification, the facilitators may require winning applicants to either pay an additional exorbitant fee or agree to enter into a marriage with another of the facilitator's paying clients solely for the purpose of extending immigration benefits.

Fraud Risks Evolve Over Time

Visa fraud has evolved and become more sophisticated over time due to unscrupulous visa applicants who adapt to State's efforts to combat fraud, increased globalization, advanced technology, and ease of travel. Fraud schemes are no longer centralized in individual countries. Criminal fraud rings, human smuggling networks, and trafficking rings work across multiple countries to circumvent State's visa process. For example, in 2009, a typical route for traffickers from India who sought religious asylum in the United States originated in New Delhi and transited through Moscow, Dubai, Sao Paulo, and Mexico before reaching Texas, according to the Assistant Regional Security Officer Investigator in New Delhi. In addition, new technologies have helped individuals and organizations adapt to State's visa security features and develop increasingly sophisticated fraud schemes. For example, high-quality micro-printing and new assembly methods have allowed imposters to duplicate State's visa security threads and serial numbers. With global access to the Internet, fraud scams used in one country or continent have quickly made their way to others, and therefore high-fraud countries and posts have shifted from year to year. For example, only 4 countries were among the top 10 countries for visa fraud in both 2005 and 2010: the Dominican Republic, Ghana, Jamaica, and Peru.[33]

[33]The other six countries among State's 2005 Fraud Ranking included: Bangladesh, El Salvador, Haiti, Honduras, Nigeria, and the Philippines.

State Has a Variety of Tools and Resources to Combat Fraud, but Does Not Have a Policy for Systematically Utilizing Domestic Anti-Fraud Resources

Consular officers rely on State's advanced information technology, fraud reports, and domestic and overseas fraud prevention resources to improve their ability to detect and deter fraud. However, State does not have a policy to systematically utilize its domestic anti-fraud resources to offset fraud workload overseas.

State Has Implemented New Technological Tools Intended to Enhance Its Visa Fraud Prevention Efforts

The Consular Affairs Office of Consular Systems and Technology has deployed several new tools to counter fraud in the visa process, including the following:

- *Online Nonimmigrant Visa Application Form, DS-160*: In the spring of 2010, State implemented the DS-160 online nonimmigrant visa application system, which requires applicants to submit all information electronically. With the collection of electronic information prior to the scheduled visa interview, State is able to research and analyze applicants' data for indicators of fraud prior to an interview with a consular officer. Overseas, State encourages Fraud Prevention Units to conduct pre-screening checks of applicants' visa history to identify aliases or discrepancies between current and previous applications.

- *Enterprise Case Assessment Service (eCAS)*: In April 2011, State released eCAS, the first centralized system for Fraud Prevention Units to track and manage their nonimmigrant and immigrant visa fraud cases. eCAS is based in the Consular Consolidated Database, and Fraud Prevention Units use it to create, develop, and resolve fraud assessments. Previously, fraud cases were either designated as "fraud confirmed" or "fraud not confirmed." With eCAS, fraud cases are now designated as "fraud confirmed," "no fraud," or "inconclusive," which allows Fraud Prevention units more flexibility to designate that some cases have a suspicion of fraud but not enough evidence to confirm fraud. In the first 5 months of the system's use, May 2011 through September 2011, 188 posts worldwide used eCAS to process over 43,000 fraud cases. According to State, in 2012 State released an eCAS module domestically that can also be used to process passport fraud cases, and State plans to extend this module overseas in 2013.

- *MATRIX*: In 2011, State released a new fraud prevention tool known as MATRIX that is accessible to Fraud Prevention Units and Diplomatic Security agents through State's Consular Consolidated Database.[34] MATRIX is a search tool that makes associations between information on a visa application and other records and data sources. MATRIX links information in the Consular Consolidated Database to other State records, USCIS records, and INTERPOL data.[35] Fraud Prevention Managers and ARSO-Is can use MATRIX to link information contained on previous visa applications and to reveal similarities across multiple applications as an indicator of fraud. For example, according to Consular Affairs officials, MATRIX found that one applicant's contact phone number in the United States matched the phone numbers used by 17 other applicants, a possible indication of fraud.

- *Diversity Visa Entry Status Check*: In 2010, State began an online verification system called the Entry Status Check that allowed all entrants of the 2010 Diversity Visa Program to electronically, individually, and privately check the status of their online submissions through a State website. This system eliminated the need for direct mailing of Diversity Visa correspondence and enhanced State's ability to combat fraud. Prior to the electronic system, notification letters were physically mailed to the address listed on the application. Unscrupulous visa agents listed their own addresses so that the notification letters were delivered to them instead of the people selected in the lottery. The agent could demand thousands of dollars from an applicant in exchange for the letter.

- *Consular Consolidated Database Search Rules to Identify Fraud Indicators*: State is currently developing a new anti-fraud tool that will automatically search visa applications for fraud indicators and alert consular officials when fraud indicators are found. For example, State may find higher rates of fraud among visa applicants who rely on services provided by a particular local visa company. Consular

[34]MATRIX stands for Match Analytics and Trusted Real-Time Identity X-Ref (or cross-reference).

[35]The International Criminal Police Organization (INTERPOL) is the world's largest international police organization that helps police understand criminal trends, analyze information, conduct operations and, ultimately, arrest as many criminals as possible, according to INTERPOL's website.

officials in that country can request that State flag future visa applications listing that visa company's name.

State Compiles Various Internal Reports to Share Information about Fraud Trends and Available Resources

State shares information between consular posts and headquarters regarding the latest fraud trends through reporting mechanisms such as validation studies, semi-annual fraud summaries, fraud digests, fraud notices, or reporting cables, Diplomatic Security monthly status reports, and Diplomatic Security program reviews.

- *Validation Studies*: State considers validation studies to be one of the best fraud-prevention tools available to consular officers. Posts conduct validation studies on visas that have been issued to determine the extent to which the visas have been misused, and posts send summaries of fraud risks to headquarters twice a year. Posts are required to conduct at least two validation studies per year, one on a visa category of the post's choosing and one on visa referrals.[36] Generally, consular officers select a sample of visa issuances and determine how many of the visa recipients departed the United States within the terms of their visas, how many remained in the United States longer than their visas allowed, and how many never traveled to the United States.[37] Validation studies help measure the accuracy of adjudication decisions, and allow Consular Affairs officials to share emerging fraud trends across posts.

- *Semi-Annual Fraud Summaries*: State guidance calls for validation studies to be incorporated into posts' Semi-Annual Fraud Summaries—reports submitted twice annually that provide input for improvements in fraud prevention guidance, training, and resources. State guidance notes that the summaries should discuss current country conditions that may contribute to fraud risks, such as the presence of organized crime networks. According to the guidance, the summaries should discuss fraud trends for nonimmigrant visas, immigrant visas, diversity visas, passports, and coordination with

[36]Visa referrals occur when State officials refer their professional contacts for expedited visa appointments, reducing their wait time for scheduling an interview with a consular officer.

[37]Since 2008, State has been given access to DHS's Arrival and Departure Information System (ADIS) to generate a sample of issued visas to conduct a validation study. In 2011, ADIS results were linked to each visa application so that consular officers could view applicants' prior travel history.

Diplomatic Security personnel, among other topics. These studies should discuss new information that may be used to establish new fraud indicators.

- *Fraud Digests*: Since September 1996, State has published a monthly newsletter called the Fraud Digest that profiles worldwide fraud trends, fraud prevention techniques, and advances in areas such as fraud prevention technology and immigration document design. The digests are accessible on the web and are shared government-wide with approximately 3,600 subscribers, as of April 2012. The main audience for the digest is domestic and overseas consular personnel and Diplomatic Security agents.

- *Reporting Cables*: State headquarters gathers and analyzes information from posts, and distributes guidance to posts through monthly reporting cables in order to update consular officers on evolving fraud trends.

- *Diplomatic Security Monthly Status Reports*: According to Diplomatic Security officials, ARSO-Is worldwide submit monthly status reports that delineate the number of hours spent on criminal investigations and training of foreign personnel. The status report also describes progress on the post's visa cases, including preliminary queries for information and arrests. The information supplements data entered into the Diplomatic Security primary case management system known as the Investigative Management System, according to Diplomatic Security officials.

- *Diplomatic Security Program Reviews*: Diplomatic Security officials told us that Diplomatic Security program reviews are internal reports that highlight best practices at posts and make recommendations for improvements. To complete the program reviews, officials from Diplomatic Security's Office of Criminal Investigations told us that they spend 2 days at each post answering standardized questions about training, pending cases, arrests, budget, and information systems, among other topics. Diplomatic Security aims to visit all posts with an ARSO-I presence once every 2 years, according to Diplomatic Security officials.

State Has Expanded Anti-Fraud Activities Conducted by KCC

Workers at the Kentucky Consular Center support Overseas Visa Adjudication

Source: State.

KCC, located in Williamsburg, Kentucky, has become an important anti-fraud resource for State. State opened KCC in October 2000, to process worldwide diversity visa applications and reduce the workload on adjudicating officers at overseas posts. According to KCC officials, the number of local employees at KCC has increased from 40 to 273, including 54 staff working within a Fraud Prevention Unit.[38] In August 2001, KCC began a pilot project to screen all nonimmigrant visa applications with facial recognition software. According to KCC officials, after the September 11, 2001 attack, State was required to store visa applications for 7 years. As a result, KCC officials began scanning old visa applications and uploading all biographic information and evidence of visa ineligibilities. All visa applicants' biographic information, including both fingerprints and digitized photographs, is checked through State's Consular Lookout and Support System database and facial recognition software.

State describes KCC as an incubator for new consular projects, and KCC is in the process of expanding anti-fraud services to posts overseas, according to KCC officials. Currently, KCC provides prescreening services for selected posts overseas. Any post may request KCC assistance in conducting research and analysis on visa applications, either on an ad-hoc basis for individual cases, or on a pilot basis for larger-scale projects. For example, since over 50 percent of all skilled worker (H-1B) and intracompany transfers (L) visas are processed in India, KCC initiated a process to verify all petitioner information contained on these types of visa applications from posts in India, according to State officials. Globally, KCC screened 81,862 H-1B and L-1 applications for fraud in calendar year 2011. In addition to H and L visas, KCC conducts prescreening on several other visa classifications that are susceptible to fraud. According to State officials, KCC screeners and fraud analysts conduct basic checks, such as verifying the legal name of the business as well as more complex research including data mining, evaluation of the petitioning organization's business viability, and phone calls to petitioning employers. Additionally, KCC fraud analysts may also refer the case to onsite Fraud Detection and National Security officers to request a visit to the proposed employment site. If derogatory information, such as a

[38]In addition to the contractors, State employs two Foreign Service Officers, two Civil Service employees, one Diplomatic Security Special Agent, and five assistants. DHS employs one Fraud Detection National Security Directorate staff member, according to KCC officials.

revocation of a prior petition, exists on a petitioning company, screeners enter all comments into the applicant's online DS-160 form, for access by the consular officer, who makes the ultimate decision to issue or deny the visa.

In fiscal year 2012, State intends to prescreen 15 percent of all worldwide nonimmigrant and immigrant visa applications prior to the visa interview, increasing to 50 percent by fiscal year 2013. To prescreen visa applications, KCC reviews and processes all sets of documents and data received from petitioners and beneficiaries. KCC employees conduct research on visa applicants and petitioners, and provide this information to consular officers overseas so that they have access to the information prior to interviewing a visa applicant in person.[39] For example, we observed a KCC analyst conducting research on a summer work and travel visa application that listed the sponsor business as a restaurant. However, the KCC analyst determined that the physical address listed on the visa application was an adult entertainment venue, a business prohibited by the program. The KCC analyst notified the interviewing post of this finding so that the adjudicating officer would have knowledge of it before the interview. KCC now prescreens the vast majority of certain visa categories that have been associated with high rates of fraud, such as summer work and travel visas. From March 2011 to April 2012, KCC analysts researched over 9,000 companies participating in the Summer Work and Travel Program and found that 13 percent of them had fraud indicators. For example, some companies did not exist, the company's phone number was invalid, or the company reported that it never expected a summer work and travel participant.

Overseas Anti-Fraud Staffing Levels and Workload Vary by Post

Anti-fraud staffing levels in Fraud Prevention Units vary widely across overseas posts, causing disproportionate workloads. State assigns personnel to Fraud Prevention Units based on input from post management and consular affairs management at headquarters. Personnel from State's Office of Fraud Prevention Programs said resource decisions for Fraud Prevention Units are driven by visa workload

[39]KCC employees do not make decisions on whether or not to issue a visa.

and other factors at posts, not by the number of fraud cases.[40] Although statistics on the number of fraud cases confirmed, unconfirmed, or inconclusive are used by posts to direct anti-fraud strategies, Consular Affairs does not use these statistics to determine the appropriate distribution of personnel to Fraud Prevention Units.

The posts with the highest numbers of suspected fraud cases in 2011 were not assigned a number of Fraud Prevention Unit staff proportionate to the number of fraud cases, as seen in table 2. For example, one entry level officer and one mid-level officer in Santo Domingo, who were assigned to Fraud Prevention Manager positions, joined five locally employed staff in the Embassy's Fraud Prevention Unit to combat the entire country's visa fraud. With approximately 7,879 cases suspected of fraud in 2011, each member of Santo Domingo's Fraud Prevention Unit investigated an average of 1,126 cases and each member of Guangzhou's Fraud Prevention Unit investigated an average of 239 cases that year.

Table 2: Type and Number of Staff Assigned to Fraud Prevention Units and Ratio of Staff to Suspected Fraud Cases, Fiscal Year 2011

Posts with highest numbers of suspected fraud cases in 2011	Level and number of Fraud Prevention Managers	Number of locally employed staff	Total Fraud Prevention Unit staff[a]	Number of suspected fraud cases[b]	Ratio of Fraud Prevention Unit staff to cases
Santo Domingo, the Dominican Republic	1 mid-level officer, 1 entry-level officer	5	7	7879	1:1126
Kyiv, Ukraine	1 mid-level officer	7	8	7675	1:959
Ciudad Juarez, Mexico	1 mid-level officer, 1 part-time or rotational officer	11	13	3620	1:278
Shanghai, China	1 mid-level officer, 2 entry-level officers	5	8	3068	1:384
Beijing, China	1 mid-level officer, 2 part-time or rotational officers	3	6	3047	1:508

[40]The consular component of State's Overseas Staffing Model uses consular workload and environmental factors to assist in the allocation of staffing resources. Workload factors include the number of immigrant, nonimmigrant, and diversity visa cases processed annually, and environmental factors include fraud and the number of third-country national applications processed, among other criteria.

Posts with highest numbers of suspected fraud cases in 2011	Level and number of Fraud Prevention Managers	Number of locally employed staff	Total Fraud Prevention Unit staff[a]	Number of suspected fraud cases[b]	Ratio of Fraud Prevention Unit staff to cases
Guangzhou, China	1 mid-level officer, 2 entry-level officers	7	10	2386	1:239
Shenyang, China	1 mid-level officer, 1 part-time officer	5	7	2350	1:336
Bogota, Colombia	1 mid-level officer, 2 entry-level officers	4	7	2293	1:328
Accra, Ghana	1 mid-level officer	3	4	1726	1:432
New Delhi, India	1 mid-level officer, 1 entry-level officer	6	8	1640	1:205

Source: GAO analysis of State data.

[a]Staffing data was gathered as of April 30, 2012.

[b]The suspected number of fraud cases is based on data from eCAS for the period of May 1, 2001 through September 30, 2011, as well as data from State's previous fraud tracking system for the period of October 1, 2010 through April 30, 2011.

State Does Not Have a Policy for Utilizing Domestic Anti-Fraud Resources to Offset Posts' Fraud Workload

According to State officials, while State plans to expand the use of KCC anti-fraud resources, there is no systematic process for overseas posts to formally request KCC prescreening assistance. State's Program Evaluation Policy notes that program evaluation is essential for planning decisions, and evaluation findings should be integrated into program strategies and policies. However, State officials told us that anti-fraud pilot programs conducted at KCC are not formally evaluated and there is no established policy for posts to access domestic anti-fraud resources.[41] Rather, KCC provides anti-fraud assistance to overseas posts on an ad-hoc basis based on informal communication.[42]

According to KCC's Director, most posts have not requested KCC's assistance because they are not familiar with all of the anti-fraud services that KCC can provide or how to request services. For example, a Fraud Prevention Manager in a high-fraud post that we visited told us that the post would like additional KCC prescreening of certain visa categories, but was unaware of how to request KCC assistance. Multiple State

[41]Although State provided us with the parameters of five KCC pilots, it was unable to provide the results of each pilot.

[42]When a post requests additional KCC assistance, KCC officials must consult with the Visa Office, in coordination with the Office of Fraud Prevention Programs, before initiating the service.

officials told us that most KCC prescreening initiatives have been due to institutional knowledge at the management level in the field. For example, all India-specific services provided by KCC were a direct result of a Consular Manager in India who was aware of the prescreening services KCC could provide.

According to the KCC Director, there are clear benefits to utilizing KCC for fraud investigations. KCC staff are fully vetted U.S. citizens with secret clearances and access to all restricted databases used in visa adjudications. In addition, both Diplomatic Security and the U.S. Citizenship and Immigration Service are represented at KCC, and are available to assist in fraud investigations. The majority of KCC staff are provided through a contractor, and the contract provides for the ability to adjust to changes in demand for services.

Although State Offers a Variety of Anti-Fraud Training Courses, Fraud Prevention Managers Are Not Required to Take Them

Although State offers anti-fraud courses in a classroom setting and online, State does not require Fraud Prevention Managers to take them. In addition, State does not track Fraud Prevention Manager enrollment in anti-fraud courses, and therefore State does not know whether the large number of entry-level officers filling fraud prevention manager positions have taken the anti-fraud courses.

State Offers a Variety of Anti-Fraud Training Courses

The Foreign Service Institute has expanded the number of courses it offers Foreign Service Officers in fraud prevention and detection, covering topics such as advanced name checking, analytic interviewing, and emotional content analysis.[43] The institute's anti-fraud training courses include the following:

- *Basic Consular Course (PC530)*: Commonly known as ConGen, PC530 is a 6-week course that all Foreign Service officers are required to take prior to their first consular tour. PC530 is also

[43]The George P. Shultz National Foreign Affairs Training Center's Foreign Service Institute is the federal government's primary training institution for officers and support personnel of the U.S. foreign affairs community.

required for any officer heading to a consular tour who has neither done consular work nor taken ConGen in the preceding 5 years. The course contains a module covering security, accountability, fraud, and ethics, which includes training in detecting and preventing fraud.

- *Fraud Prevention for Consular Managers (PC541)*: This course is designed for Fraud Prevention Managers who are currently serving in the field, emphasizing anti-fraud and counterterrorism tools for consular officers.[44]

State also offers consular officers distance learning or online courses in detecting and preventing fraud. These courses are either prescheduled live courses, prerecorded or accessible 24 hours a day, or offered on-demand. Online consular training in fraud includes the following:

- *Detecting Imposters (PC128)*: This course teaches students procedures for identifying imposters either at the interview window or in photographs.

- *Detecting Fraudulent Documents (PC544)*: This course teaches consular officers how to determine whether a document has been altered or is counterfeit.

- *New Consular Technologies (eCAS and MATRIX)*: This course trains consular officers in how to use eCAS and MATRIX to combat visa fraud.

State officials from the Office of Consular Systems and Technology said that its training programs are updated as soon as new features are rolled out, and the training typically focuses on new technology features. Consular officers are provided with manuals that explain the new software tools about a month in advance and can attend live and prerecorded training courses. While some consular courses can take about 2 hours, training in MATRIX is a prerecorded session that takes approximately 30 minutes. Although training on new technological tools is available and encouraged by State, a survey of Fraud Prevention Managers revealed

[44]The Foreign Service Institute also offers PC542, a fraud prevention course for locally employed staff.

that respondents' lack of knowledge of some key anti-fraud tools indicated that updates were not uniformly reaching officers.[45]

State Does Not Require Fraud Prevention Managers to Take Anti-Fraud Courses

While State encourages Fraud Prevention Managers to take updated fraud prevention training, the training is not required. Entry-level officers are required to complete 6 weeks of basic consular training prior to their arrival at post but are not required to take other advanced anti-fraud courses offered at the Foreign Service Institute or online, such as eCAS or MATRIX. For example, four of the five Fraud Prevention Managers we met with had not been trained in MATRIX. Advanced fraud training courses are targeted to mid-level officers, but the majority of Fraud Prevention Manager positions (180 of 222) were filled by an entry-level officer or an officer of unspecified grade. In 2011, a little more than half of the students enrolled in PC541 were entry-level officers, and State could not determine whether Fraud Prevention Managers were among them. Additionally, between October 2009 and July 2012, entry-level officers made up approximately 22 percent (489 of 2,252) of the total number of students who registered for Detecting Imposters (PC128) and 21 percent (486 of 2,246) of the total number of students who registered for Detecting Fraudulent Documents (PC544). Without advanced fraud training courses, Fraud Prevention Managers may not know about the roles and responsibilities of KCC, or how to use the Consular Lookout and Support System name-check database and biometric systems. For example, two of the five Fraud Prevention Managers with whom we met were unfamiliar with the anti-fraud services available at KCC. According to the Office of Fraud Prevention Program's country desk officers, the level of anti-fraud training offered to Foreign Service Officers largely depends on the officer's experience level, years in the Foreign Service, and available time. Desk officers offer a 1-hour briefing of country-specific fraud issues and resources to all Foreign Service Officers prior to their deployment, but not all of the officers take advantage of the briefing, according to officials from the Office of Fraud Prevention Programs.

In addition, a significant period of time may pass between an entry-level officer's completion of the basic consular course and the time when he or she assumes the role of Fraud Prevention Manager. Entry-level officers

[45]State's survey reached 158 of the 222 visa-issuing consular posts. We determined the results to be sufficiently reliable for our purposes.

are required to take only limited fraud prevention training that does not include new anti-fraud technologies. For example, officers may not arrive at a post until they complete required language training, which can take 6 months to a year. Additionally, entry-level officers who are not on the consular affairs career track may serve a rotation in a different specialty area before serving a rotation in consular affairs. Finally, many entry-level officers are not assigned to the Fraud Prevention Manager position until after they arrive at post.

State Does Not Track Enrollment of Fraud Prevention Managers in Anti-Fraud Courses

While State offers these anti-fraud training courses, both in Washington D.C., and online, it does not track whether Fraud Prevention Managers are taking them. In 2012, four of the five Fraud Prevention Managers with whom we met had not been formally trained in MATRIX.[46] Since its rollout, State has not tracked the number of Fraud Prevention Managers that have been trained in eCAS and MATRIX. In addition, State was unable to differentiate enrollment data by position and therefore could not confirm that Fraud Prevention Managers had enrolled in any fraud prevention course.

Conclusion

State's fraud prevention efforts protect the integrity of the visa process and help prevent people from exploiting the visa process to commit crimes or threaten the security of the United States. Fraud trends evolve over time as criminal networks and unscrupulous visa applicants seek to circumvent State's visa application process. Meanwhile, the number of visas issued has risen steadily since 2003 and consular officers face increased pressure to expedite visa processing. The evolving nature of fraud and increases in the volume of visas adjudicated require State to continuously update its anti-fraud efforts. In recent years, State has taken steps to enhance the tools and services available to combat visa fraud, including the deployment of new anti-fraud technologies and resources improving State's ability to prescreen applications for indicators of fraud and to readily access information from prior visa applications. However, these technologies and resources are only useful if consular officers know that they exist and know how to use them. Currently, the majority of Fraud Prevention Manager positions are filled by entry-level officers, who are

[46]The lack of training is a trend that has continued since at least 2005, when we reported that 10 of the 25 consular managers with whom we met said that their Fraud Prevention Managers had not yet received training specific to their fraud prevention duties.

not the targeted audience for advanced anti-fraud training, and State does not require them to be trained in all anti-fraud technologies. As a result, Fraud Prevention Managers may not be fully equipped to detect and combat fraud. Furthermore, posts increasingly rely on KCC to prescreen certain visa applications for fraud, and State intends to prescreen 50 percent of all visa applications worldwide prior to consular interviews. However, State does not have a policy that specifies how to systematically utilize the center's resources, based on post workload and fraud trends. Therefore, State cannot be assured that a valuable tool to combat fraud is being strategically utilized. Absent effective support and training, Fraud Prevention Units may make uninformed decisions, thus enabling ineligible aliens, including potential terrorists, to gain admission to the United States.

Recommendations

To further improve the visa fraud prevention process, we recommend that the Secretary of State take the following two actions:

(1) Formulate a policy to systematically utilize anti-fraud resources available at the Kentucky Consular Center, based on post workload and fraud trends, as determined by the department; and

(2) Establish standardized training requirements for Fraud Prevention Managers, to include training in advanced anti-fraud technologies, taking advantage of distance learning technologies, and establishing methods to track the extent to which requirements are met.

Agency Comments

We provided a draft of our report to State and DHS. State and DHS provided technical comments, which we incorporated as appropriate. State also provided written comments, which are reproduced in appendix IV. State concurred with our recommendations.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 14 days from the report date. At that time, we will send copies of this report to interested members of Congress and the Secretaries of Homeland Security and State, as well as other interested members of Congress. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8980 or CourtsM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Michael J. Courts,
Acting Director, International Affairs and Trade

Appendix I: Scope and Methodology

This report examines (1) countries and visa categories subject to the most visa fraud; (2) technologies and resources to combat fraud; and (3) training requirements of State officials responsible for fraud prevention. This report focuses on visa fraud, and not passport fraud.[1]

To determine the countries and visa categories subject to the most visa fraud, and the evolution of fraud over time, we reviewed nonimmigrant and immigrant visa issuance data from the Consular Consolidated Database from 1992 to 2011. While we did not analyze State data on the number of visa applications during this time period, we reviewed visa refusal percentages by country. We did not review the reliability of these data because they were for background purposes only. We also reviewed State Fraud Digest reports from September 1996 through May 2012, semi-annual fraud summaries for some of the posts with the highest numbers of suspected fraud cases, and Diplomatic Security Monthly Status reports from fiscal year 2011. We also analyzed fiscal year 2010 and 2011 data on the number of visa applications referred to Fraud Prevention Units. We found 2010 data more reliable because State transitioned to a new fraud management system in the middle of fiscal year 2011, and formal guidance on how and when to refer cases to Fraud Prevention Units was not released until July 2012. We compared the 2005 Country Fraud Ranking of Posts to fiscal year 2010 data on the countries with the highest numbers of suspected fraud cases. We found these data to be sufficiently reliable for the purposes of indicating the countries that reported the highest volumes of reported fraud cases and made the most referrals. However, we found that these data may not accurately reflect the relative levels of actual fraud in each country due to possible differences in reporting by posts. We used fiscal year 2010 data for our analysis because State introduced a new data system in 2011, and we noted some potential problems with the 2011 data that arose due to the transition. State officials in the Office of Fraud Prevention Programs provided qualitative information on the types of visa categories that are subject to fraud. Lastly, we interviewed State officials at headquarters and abroad to discuss recent fraud trends.

[1]In March 2009, a GAO investigation exposed major vulnerabilities in State's passport issuance process, demonstrating that terrorists or criminals could steal an American citizen's identity, use basic counterfeiting skills to create fraudulent documentation for that identity, and obtain a genuine U.S. passport. GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C.: Mar. 13, 2009).

To assess State's use of technologies and resources to combat fraud, we met with State's Bureau of Consular Affairs Office of Consular Systems and Technology to review State's major data systems as well as the latest technological tools available to consular officers and Fraud Prevention Managers. Specifically, we received demonstrations on State's newly deployed Enterprise Case Assessment Service (eCAS) used for tracking fraud cases, and MATRIX, a search tool used in fraud prevention. We visited the Kentucky Consular Center, an anti-fraud resource available to posts, and observed its activities. We interviewed State officials at posts regarding their usage of these tools and resources. To determine the reliability of data captured by eCAS on the number of cases referred to Fraud Prevention Units and the number of confirmed cases, we met with consular officers and Fraud Prevention Managers in five posts to determine how information was entered into eCAS. We determined that the eCAS system was widely used across posts and was sufficiently reliable to determine the general volume of fraud referrals.

To understand the training required of State officials responsible for combating fraud, we gathered information about training requirements and course enrollment from the Foreign Service Institute's Student Training Management System. We interviewed Foreign Service Institute personnel regarding controls, strengths and limitations of the course enrollment data and determined it was sufficiently reliable for our purposes. We also analyzed data on the number of direct hire and local staff working in all 222 visa-issuing consular posts as of December 2011 and reviewed data gathered by State liaisons from the Consular Workload Statistics System on the number and grade of officers assigned to Fraud Prevention Units at consular posts as of April 2012. We obtained staffing data from State's GEMS database. We tested the data on direct hires and local staff working at visa-issuing posts for completeness, confirmed the general accuracy of the data with select overseas posts, and interviewed knowledgeable officials from the Office of Resource Management and Organizational Analysis concerning the reliability of the data. We assessed data on the number and grade of officers assigned to Fraud Prevention Units for reliability, and interviewed Consular Affairs officials regarding how the data was collected and entered into the database, the controls and reviews of the data collection, and the major strengths and limitations of the data. We found the data to be sufficiently reliable for our purposes. Lastly, we conducted interviews with visa chiefs, Fraud Prevention Managers, and DS Assistant Regional Security Officers working in five overseas posts on issues related to consular staffing and resources, among other topics.

We visited U.S. consular posts in five countries—Brazil, the Dominican Republic, India, Jordan, and Ukraine. During these visits, we observed visa operations and interviewed consular staff and embassy management about visa adjudication policies, procedures, and resources. In addition, we spoke with officials from other U.S. agencies that assist consular officers in the visa adjudication process. We chose Brazil, the Dominican Republic, India, and Ukraine because each of the fraud prevention teams in these countries investigated 500 or more fraud cases in fiscal year 2010. We chose Jordan because of the nature of the fraud cases investigated in that country, which included security concerns.

We conducted our work from August 2011 through September 2012, 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.

Appendix II: U.S. Nonimmigrant Visa Classes of Admission

Foreign nationals seeking to enter the United States temporarily may apply for entry under the following visa classes of admission:

Visa Class	Description
Transit aliens	
C-1	Aliens in continuous and immediate transit through the United States
C-2	Aliens in transit to the United Nations Headquarters District
C-3	Foreign government officials, attendants, servants, and personal employees, and spouses and children in transit
Temporary visitors for business	
B-1	Temporary visitors for business
GB	Visa Waiver Program—temporary visitors for business to Guam
WB	Visa Waiver Program—temporary visitors for business
Temporary visitors for pleasure	
B-2	Temporary visitors for pleasure
GT	Visa Waiver Program—temporary visitors for pleasure to Guam
WT	Visa Waiver Program—temporary visitors for pleasure
Temporary workers and trainees	
H-1B	Temporary workers with “specialty occupation”
H-1B1	Chile and Singapore Free Trade Agreement Aliens
H-1C	Nurses under the Nursing Relief for Disadvantaged Areas Act of 1999
H-2A	Seasonal agricultural workers
H-2B	Seasonal nonagricultural workers
H-3	Trainees
H-4	Spouses and children of H-1, H-2, or H-3 visa holders
O-1	Temporary workers with extraordinary ability or achievement in the sciences, arts, education, business, athletics, TV or film.
O-2	Temporary workers with essential skills accompanying and assisting O-1 visa holders
O-3	Spouses and children of O-1 and O-2 visa holders
P-1	Temporary workers—internationally recognized athletes or entertainers for a specific competition or performance
P-2	Temporary workers—artists or entertainers under reciprocal exchange programs with a similar organization of a foreign state
P-3	Temporary workers—artists or entertainers under culturally unique programs
P-4	Spouses and children of P-1, P-2, or P-3 visa holders
Q-1	Temporary workers in international cultural exchange programs
R-1	Temporary workers in religious occupations

Visa Class	Description
R-2	Spouses and children of R-1 visa holders
TN	North American Free Trade Agreement (NAFTA) professional workers
TD	Spouses and children of TN visa holders
Treaty traders and investors	
E-1	Treaty traders and spouses and children
E-2	Treaty investors and spouses and children
E-3	Australian Free Trade Agreement principals and spouses and children
Intracompany transferees	
L-1	Intracompany transferees
L-2	Spouses and children of L-1 visa holders
Representatives of foreign information media	
I-1	Representatives of foreign information media and spouses and children
Students	
F-1	Students—academic institutions
F-2	Spouses and children of F-1 visa holders
F-3	Canadian or Mexican national commuter students—academic institutions
M-1	Students—vocational/nonacademic institutions
M-2	Spouses and children of M-1 visa holders
M-3	Canadian or Mexican national commuter students—vocational/nonacademic institutions
Exchange visitors	
J-1	Exchange visitors
J-2	Spouses and children of J-1 visa holders
Other categories	
A-1	Ambassadors, public ministers, career diplomatic or consular officers, and spouses and children
A-2	Other foreign government officials or employees and spouses and children
A-3	Attendants, servants, or personal employees of A-1 and A-2 visa holders and spouses and children
BE	Bering Strait Agreement aliens
FSM	Federated States of Micronesia nationals
G-1	Principal resident representatives of recognized foreign member governments to international organizations, staff, and spouses and children
G-2	Temporary representatives of recognized foreign member governments to international organizations and spouses and children
G-3	Representatives of unrecognized or nonmember foreign governments to international organizations and spouses and children

Visa Class	Description
G-4	Officers or employees of unrecognized international organizations and spouses and children
G-5	Attendants, servants, or personal employees of G-1, G-2, G-3, or G-4 visa holders and spouses and children
K-1	Alien fiancés(ees) of U.S. citizens
K-2	Children of K-1 visa holders
K-3	Alien spouses of U.S. citizens
K-4	Children of K-3 visa holders
MIS	Republic of the Marshall Islands nationals
N-1 to N-7	North Atlantic Treaty Organization (NATO) aliens, spouses, and children
N-8	Parents of international organization special immigrants
N-9	Children of N-8 visa holders or international organization special immigrants
PAL	Republic of Palau nationals
Q-2	Irish Peace Process Cultural and Training Program aliens
Q-3	Spouses and children of Q-2 visa holders
T-1 to T-5	Victims of a severe form of trafficking and spouses, children, parents, and siblings
U-1 to U-4	Aliens suffering physical or mental abuse as victims of criminal activity and spouses, children, and parents
V-1 to V-3	Spouses and children of a lawful permanent resident who has been waiting 3 years or more for immigrant visas and dependents

Source: State.

Appendix III: Case Studies

The following five case studies provide examples of the types of activities carried out by Fraud Prevention Units and Assistant Regional Security Officer Investigators (ARSO-Is) overseas.

Fraud Prevention Unit Case Study

In Ukraine, we observed consular officers adjudicating visas for the Summer Work and Travel program. A consular officer suspected an applicant's student identification was fraudulent, and he told the applicant to wait while he asked the Fraud Prevention Unit for assistance. The senior Locally Employed Staff (LES) person inspected the student ID and said it was most likely a fake. The consular officer asked the LES to assist in questioning the applicant. The LES reviewed the applicant's school transcripts that were submitted with the visa application, and asked the applicant to provide the name of the school's chancellor. The applicant could not provide the name. The Fraud Prevention Unit called the school to attempt to verify whether the applicant was currently enrolled, but the school would not verify the applicant's status. The Fraud Prevention Unit told the consular officer that they believed the applicant was committing fraud on her application, and the consular officer denied the visa.

ARSO-I Case Studies

U.S. Embassy Santo Domingo, the Dominican Republic

U.S. Major League Baseball (MLB) teams award large signing bonuses to younger prospective players in the Dominican Republic, creating a significant economic incentive to make prospective players seem younger. As a result, MLB prospects often falsify their ages and sometimes their identities on visa applications to make them appear younger than they truly are. To date, ARSO-I Santo Domingo has facilitated the arrests of two MLB Dominican talent scouts, an MLB Investigator, and an MLB pitcher, among others, for participating in identity fraud. The pitcher, a Dominican citizen, assumed the identity of a younger person and obtained a contract to play professional baseball as a pitcher in the United States in 1999. The pitcher has since illegally obtained at least 10 nonimmigrant visas in his assumed identity. ARSO-I Santo Domingo confirmed the pitcher's true identity and coordinated with the Dominican prosecutors' office to obtain a Dominican arrest warrant. The pitcher later returned to the Dominican Republic and obtained travel documents and a new nonimmigrant visa petition from the MLB in his true identity, and applied for a nonimmigrant visa. The interviewing consular officer found the pitcher ineligible for the nonimmigrant visa due to identity fraud, and the ARSOI-I Santo Domingo subsequently facilitated his arrest

by the Dominican National Police, based on his outstanding Dominican arrest warrant.

U.S. Consulate Sao Paulo, Brazil

In December 2010, Sao Paulo Civil Police arrested a Brazilian who presented false documents in support of his U.S. visa application. This was the ninth arrest of applicants whom had named the same individual known to be a smuggler and fraudulent document vender on their visa application. Further investigation identified approximately 70 persons who had used false documents provided by the document vendor since 2009. ARSO-I Sao Paulo received information that the document vendor and his accomplices were also producing false documents in support of Canadian visa applications, and Italian and Brazilian passports. In March 2011, the Brazilian Federal Police, the State of Santa Catarina Civil Police, and the State of Santa Catarina Prosecutor's office arrested the document vendor and three of his accomplices.

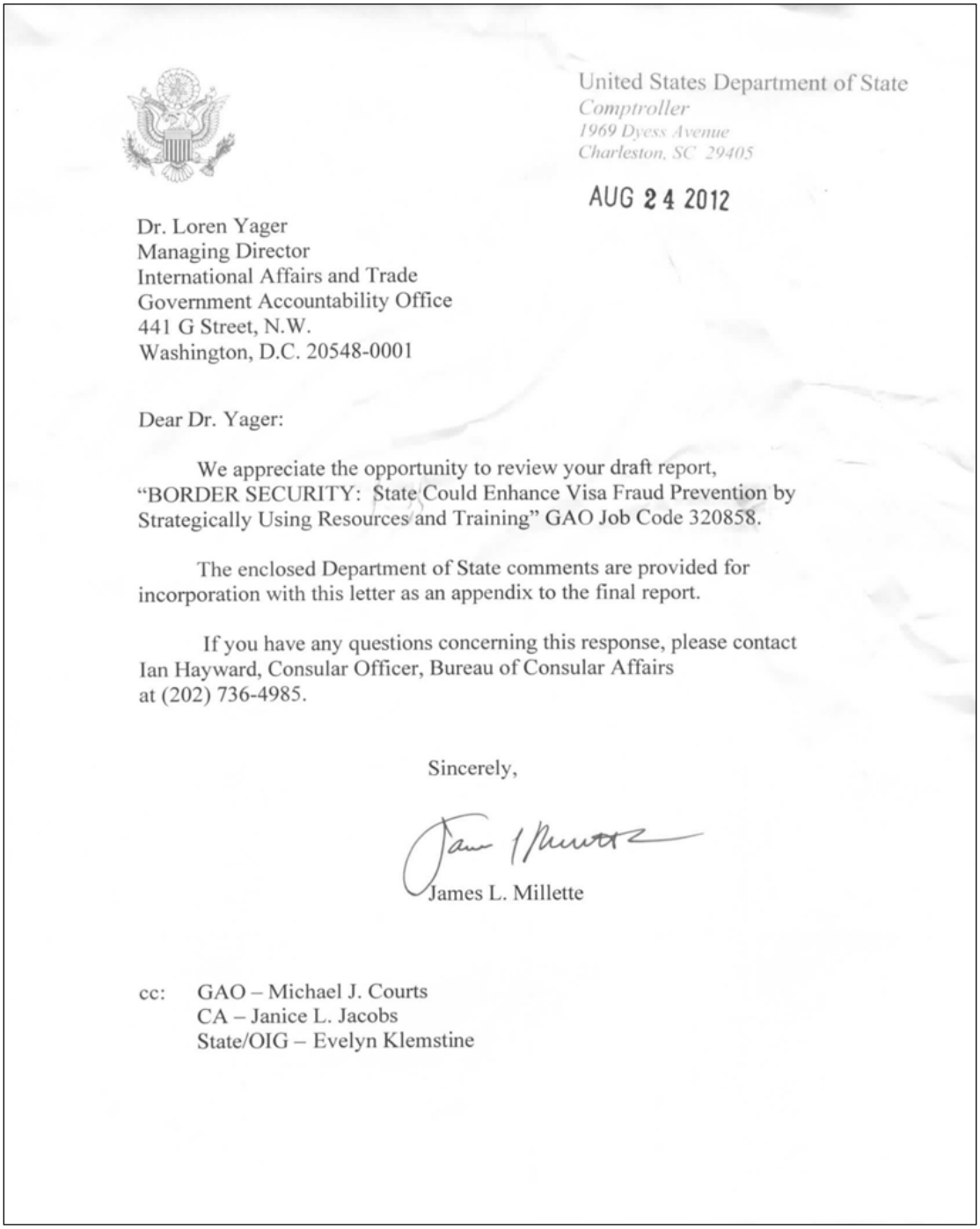
U.S. Embassy New Delhi, India

Immigrations Customs Enforcement (ICE) contacted the Deputy Assistant Regional Officer Investigator in New Delhi after receiving information that a private translator was extorting money from U.S. Citizenship and Immigration Services (USCIS) refugee/asylum applicants. The translator had access to protected information from USCIS files. ICE spoke with an informant who was being threatened by the translator to pay significant sums or have her application denied. Preliminary investigations determined that the translator would "cold-call" asylum applicants. ARSO-I New Delhi and ICE interviewed the translator, three USCIS local employees, and three local guards. The translator denied obtaining personal identifiable information from embassy staff. As a result of this investigation, the translator was arrested upon departure of the Embassy, one local guard was terminated for accepting money from the translator, and one USCIS LES employee was put on administrative leave for divulging personally identifiable information.

U.S. Embassy Kyiv, Ukraine

Immigration Customs Enforcement (ICE) Attaché contacted ARSO-I Kyiv for assistance with an individual present in Kyiv with an active INTERPOL Red Warrant for human trafficking. The fugitive was wanted in the Eastern District of Michigan for forced labor, money laundering, immigration and visa fraud, and witness tampering. ARSO-I Kyiv coordinated assistance with the Ministry of Internal Affairs Organized Crime Department. The Ukrainian Ministry of Internal Affairs Organized Crime Department agents arrested the fugitive at his residence for immigration overstay charges. ARSO-I Kyiv and ICE Attaché Frankfurt escorted the fugitive from Kyiv to New York, where the fugitive was arrested by ICE agents.

Appendix IV: Comments from the U.S. Department of State



United States Department of State
Comptroller
1969 Dyess Avenue
Charleston, SC 29405

AUG 24 2012

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "BORDER SECURITY: State Could Enhance Visa Fraud Prevention by Strategically Using Resources and Training" GAO Job Code 320858.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Ian Hayward, Consular Officer, Bureau of Consular Affairs at (202) 736-4985.

Sincerely,

James L. Millette

cc: GAO – Michael J. Courts
CA – Janice L. Jacobs
State/OIG – Evelyn Klemstine

Department of State Comments on GAO Draft Report

BORDER SECURITY: State Could Enhance Visa Fraud Prevention by Strategically Using Resources and Training
(GAO-12-888, GAO CODE 320858)

The Department thanks GAO for its evaluation of the Department's visa fraud prevention efforts. The Department appreciates GAO's recognition of the variety of technological tools and resources we have developed to assist consular officers in combating fraud, including those rolled out in the recent past. The Department also appreciates GAO's recognition of the value of fraud prevention training offered at the Foreign Service Institute and of the increasingly important role played by Kentucky Consular Center (KCC) in prescreening visa cases.

The Department wishes to address an omission. On page 26, the GAO proffers a conclusion, stating that the Department has made strides in its effort to combat fraud and listing recent State initiatives which contribute to strengthening the fraud prevention program. The GAO fails to include Diplomatic Security's contribution to this improvement. The amount of resources and personnel dedicated to the Assistant Regional Security Officer Investigator (ARSO-I) program has more than doubled over the past four years. In 2008, there were 40 ARSO-Is assigned to consular sections worldwide. There are currently 84, and by the summer of 2013, DS will have 105 ARSO-Is at 93 posts in 63 countries. The GAO also focuses almost solely on nonimmigrant visas and does not mention the immigrant visa and nonimmigrant-K-visa fraud prevention prescreening efforts of the National Visa Center (NVC) in Portsmouth, New Hampshire.

The Department also points out that since some developments in the report are recent, including the rollout of ECAS in April 2011 and its phased adoption at posts, many individuals in the field have not yet received classroom-based training. Such training has now been incorporated as part of the Automation for Consular Managers and Fraud Prevention for Consular Managers training courses. Additional guidance and information on corresponding training regarding new systems was also provided through recent cables (including a July 2012 cable on using ECAS) within the period of the study.

Recommendation 1: *Establish requirements for FPM training in advanced anti-fraud technologies and track the extent to which requirements are met.*

-2-

The Department agrees with this recommendation. The Bureau of Consular Affairs will work with FSI to establish requirements and to create a tracking mechanism.

Recommendation 2: *Formulate a policy on when and how to utilize KCC anti-fraud resources.*

The Department agrees with this recommendation. The Bureau of Consular Affairs in coordination with Diplomatic Security will draft and disseminate the policy guidance. (ok)

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Michael J. Courts, (202) 512-8980 or CourtsM@gao.gov

Staff Acknowledgments

In addition to the individual named above, Anthony Moran (Assistant Director), Jon Fremont, Julia Ann Roberts, Katie Bernet, Karen Deans, Martin De Alteriis, Etana Finkler, Mary Moutsos, Mark Speight, and Maria Stattel made key contributions to this report. Others providing technical assistance include Claude Adrien and Emily Biskup.