United States General Accounting Office

GAO

Report to the Chairman, Committee on International Relations, House of Representatives

May 1996

PASSPORTS AND VISAS

Status of Efforts to Reduce Fraud

G A O
75 years
1921 - 1996

GAO

United States
General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division

B-260437

May 9, 1996

The Honorable Benjamin A. Gilman
Chairman, Committee on International Relations
House of Representatives

Dear Mr. Chairman:

In light of the growing problem of illegal immigration, the Department of State developed a comprehensive strategy to make its visa and passport operations more efficient and less vulnerable to fraud. This report assesses (1) the status of the key initiatives the Department of State planned to implement this strategy and (2) compliance with internal management controls by consular staff at selected posts overseas. We conducted our review to comply with our basic legislative responsibilities and are sending this report to your committee because of its long-standing interest in this subject.

Background

Since 1987, State has recognized that the lack of adequate controls over visa processing is a material weakness that increases U.S. vulnerability to illegal immigration and diminishes the integrity of the U.S. visa. Specific problems have included (1) inadequate management controls, (2) lax security over visas, (3) unreliable equipment, and (4) unsupervised staff. State has acknowledged that it cannot eliminate all attempts to commit fraud, but it can make it more difficult for fraud to occur by improving the security features of the visa, expanding and improving automated systems, and strengthening staff supervision.

State's Inspector General's 1993 investigation of the issuance of visas to an ineligible visa applicant, who was subsequently convicted of conspiracy to commit terrorist acts in the United States, highlighted the need for improved internal communications at the overseas posts. In an attempt to address this problem, State established embassy committees designed to promote closer cooperation with other agencies in identifying individuals ineligible for visas.

Since 1990, State has reported that the passport process is a material weakness and vulnerable to fraud, including employee malfeasance. According to State, fraudulently obtained passports are being used to enter the country illegally and create false identities to facilitate criminal activities such as narcotics and weapons trafficking, smuggling children for use in pornography, and flight to avoid prosecution from criminal charges. In an attempt to address the problem, State is redeveloping and upgrading its systems to provide comprehensive accountability and improved internal controls.

We visited nine overseas posts to ascertain the extent to which State has implemented controls over passport and visa operations: Canberra and Sydney, Australia; London, England; Guatemala City, Guatemala; Tokyo, Japan; Nairobi, Kenya; Seoul, Korea; Mexico City, Mexico; and Johannesburg, South Africa.

Results in Brief

Efforts to overcome the material weaknesses in visa and passport processing have had mixed results. After initial delays, State has made steady progress in installing its machine-readable system—the primary initiative for eliminating visa fraud—and provided all visa-issuing posts with automated access to its global database containing names of individuals ineligible for a visa. However, operational problems have diminished the effectiveness of these efforts. These problems include (1) technical problems that have limited the availability and usefulness of the visa improvements, (2) limited usefulness of embassy lookout committees because of the reluctance of some agencies to share information and the lack of representation of key agencies, and (3) lack of compliance with management control procedures designed to decrease the vulnerability of consular operations to fraud.

State is behind schedule in its modernization and enhancement efforts designed to reduce passport fraud. State originally planned to have installed a new wide-area network, developed a system to print a digitized passport photograph, and completed installation of a system to verify the multiple issuance of passports by December 1995. However, only the installation of the wide-area network, upon which the other two projects depend, has been completed. Full implementation also depends on the completion of the modernization of the passport production system, which State indicates is dependent on the availability of funding. State's current goal is for full implementation by the end of calendar year 1996.

Technical Problems Reduce Effectiveness of Visa Automation

In 1989, State began the machine-readable visa program as its primary initiative for eliminating fraudulent nonimmigrant visas. The machine-readable visa is considered a more secure document than its predecessor because the new visa is printed on synthetic material that is more secure than paper, is attached to the passport, and has a machine-readable zone with an encryption code. At the ports of entry, the Immigration and Naturalization Service and U.S. Customs Service can check names by scanning the machine-readable zone of the visa. The visas also include a digitized photograph of the traveler.

State introduced the machine-readable visa system in 1989. The original due date for installation of the system was 1991, but installation was delayed for 15 months for additional review and analysis of the program. State set a new goal of 1995 to complete installation. However, State's Inspector General reported that State had not received sufficient funds to meet this goal. In 1994, after the World Trade Center bombing, the Congress directed State to install automated lookout systems at all visa-issuing posts by October 30, 1995. State also made a commitment to install the machine-readable visa system at all visa-issuing posts by the end of fiscal year 1996. The Congress authorized State to retain $107.5 million through fiscal year 1995 in machine-readable visa processing fees to fund these and other improvements.

As of December 1995, State had installed its machine-readable visa system at 200 posts, and all of the posts had automated access to the Consular Lookout and Support System (CLASS) either through direct telecommunications lines to the CLASS database in Beltsville, Maryland, or via the distributed name check (DNC) system, a stand-alone personal computer system with the CLASS database on tape or compact disk. By the end of fiscal year 1996, all posts are expected to have the machine-readable visa system, be on line with CLASS, and have the DNC as a backup, according to the Bureau of Consular Affairs. State will continue to upgrade the system's software and hardware and pilot test a new version of the system. State spent a total of about $32 million on the installations in fiscal years 1994 and 1995 and plans to spend another $45 million through fiscal year 1998.

Although most posts now have automated name-check capability and machine-readable visa systems, technical problems have limited their usefulness and availability. Posts often experience transmission problems with the telecommunications lines that support the system. U.S. embassies in Mexico City, Guatemala City, Sydney, Nairobi, and Seoul, which have direct access to CLASS, have experienced problems with the telecommunications lines and interruptions of CLASS. These disruptions have resulted in considerable delays in visa issuance and weakened visa controls. For example, during our visit to Mexico City we noted that consular staff were using the old microfiche system to check names during telecommunications disruptions rather than the DNC that was designed as backup. They used the microfiche system because using the DNC to check names was often a slow process. By using the microfiche system, the post ran the risk of approving a visa for an applicant who had been recently added to CLASS but had not yet been added to microfiche.

State's Diplomatic Telecommunications Service Program Office works with the international telecommunications carriers to find solutions where possible. However, according to an official of that office, if the problem is in the telecommunications lines of the host country, little can be done except to improve the post's backup system. The Bureau of Consular Affairs has developed a new version of the software for the DNC to serve as a faster, more reliable backup when used with a new computer. The DNC software and new personal computers were sent to over 30 high-volume posts in 1995, according to a Bureau official.

Lack of Cooperation Limits Usefulness of Terrorist Lookout Committees

In the aftermath of the World Trade Center bombing, State directed all diplomatic and consular posts to form committees with representatives from consular, political, and other appropriate agencies to meet regularly to ensure that the names of suspected terrorists and others ineligible for a visa are identified and put into the lookout system. Of the nine posts we visited, all but Sydney and Johannesburg had terrorist lookout committees, and those two posts were represented by the lookout committees at their embassies in Canberra and Pretoria, respectively.

Embassy officials at two of the nine posts we visited questioned the value of the committees, mainly because of the lack of cooperation from some agencies. Some agency representatives have been reluctant to provide to the consular sections the names of suspected terrorists, or others the U.S. government may want to keep out of the country, due to the sensitivity of the information and restrictions on sharing information. Officials from one of the law enforcement agencies contacted expressed concern that the information entered into CLASS could be traced to the originating agency and compromise its work. Only one of the agency officials we interviewed said that he had seen guidance from his agency on the extent to which this agency could share information. In addition, not all agencies are represented on these committees. For example, according to a consular official, the committee in Pretoria does not include representatives from the Federal Bureau of Investigation, the Customs Service, and the Drug Enforcement Agency.

Consular officials have pointed out that the lookout committees are intended to augment rather than replace coordination activities at headquarters. Additionally, according to consular officials, they are (1) working closely with individual posts to resolve coordination problems, (2) maintaining close liaison with participating agencies at the headquarters level to ensure continued cooperation and commitment, and (3) soliciting increased participation from agencies whose contributions were limited in the past. State says that it has also taken steps to clarify terrorist reporting channels.

Overseas Posts Do Not Always Adhere to Internal Controls

The posts we visited did not routinely comply with State's own internal control procedures. These procedures are described fully in the Department's Management Control Handbook and summarized for consular officers in the Consular Management Handbook. One common shortcoming was the use of Foreign Service Nationals (FSN) to check names through CLASS without the direct supervision of a U.S. officer. Other shortcomings were the lack of security over controlled equipment and supplies and the failure to report and reconcile daily activities and follow cashiering procedures.

Unsupervised Name Checks

According to the Consular Management Handbook, depending on the volume of visa fraud at a post, the embassy may assign the name check function to U.S. employees or assign a U.S. employee to monitor FSN staff doing name checks. Failure to check names could lead to issuance of visas to individuals who are ineligible. In June and July of 1993, the Inspector General testified that an individual convicted of conspiracy to commit terrorist acts in the United States was able to obtain a visa even after his name was added to the lookout system because consular staff failed to do the required name check. The Inspector General further testified that adequate controls were not in place to ensure that name checks were done.

FSNs were responsible for checking names at five of the posts we visited. Of those posts, Johannesburg, Sydney, and Tokyo were not equipped with the machine-readable visa system. The consular officers at these posts relied on the FSNs to notify them when an applicant's name matched one in the CLASS database. FSNs in Johannesburg were not required to annotate the visa applications to show that the applicants' names had been checked. Thus, the consular officers lacked any assurance that the FSNs actually checked the names or advised the consular officers of all matches.

Consular officers in Tokyo and Sydney said they periodically reviewed the visa applications and observed FSNs. One of the officials acknowledged that consular officers rely more heavily on FSNs than strict adherence to State Department guidance might suggest. However, the officials did not believe the reliance on FSNs was a problem because of the low risk of fraud at their posts.

Installation of the machine-readable visa system should help rectify this situation. Unless an American officer overrides it, the system provides the results of the name check for the American officer's review. Moreover, Bureau officials believe improved procedures and software enhancements to take effect on April 30, 1996, will make unsupervised name checks impossible. Consular officers will be required to certify in writing that they have checked the automated lookout system and that there is no basis for excluding the applicant.

Inadequate Physical Security

Three of the nine posts we visited demonstrated a lack of physical security over visa equipment and supplies. Without adequate controls, funds, equipment, and supplies can be misappropriated or misused. For example, during our fieldwork at the consulate in Johannesburg, access to the nonimmigrant visa processing area was not physically restricted, and personnel from other sections of the embassy were observed traversing the consular section to reach other parts of the embassy. In addition, the safe containing visa supplies was left unsecured on several occasions, and refused visa applications were not stored in a locked storage case as required.

Daily Activities Not Routinely Reconciled

Two of the posts we visited reported problems with using required reports to reconcile their daily activities. State's nonimmigrant visa reconciliation procedures require the posts to (1) maintain a log of visa numbers issued and spoiled, (2) inspect spoiled visas before entering them in the log, (3) ensure that each application was approved by an authorized officer, and (4) verify that each number in the visa number series is accounted for. The failure to follow these procedures provide obvious opportunities for fraud.

Consular officials in Seoul said they could not use the reports generated by the nonimmigrant visa processing system to reconcile the number of visas issued to the number of used foils.[1] The consular officials believed

[1] "Foils" are the blanks upon which the visas are printed.

this was because the system was designed for posts that accept, adjudicate, and issue visas on the same day, and posts as large as Seoul could not produce visas in one day. As a result, they said that they had developed their own system of accounting for visa foils. We also observed reconciliation problems in Sydney.

Cashiering Procedures Not Always Followed

Three of the posts we visited also failed to comply with established cashiering procedures such as reconciling services rendered with collections received. Routine reconciliations are an essential tool in detecting employee malfeasance. In Nairobi, neither the accountable officer nor the budget and fiscal officer reconciled collections with services. They said they were unaware of the requirement. In Johannesburg, the accountable officer was reconciling fees collected with services rendered, but was not conducting periodic unannounced cash audits as required in the Consular Management Handbook. The accountable officer for passport operations at the U.S. Embassy in Mexico City also had not conducted periodic cash audits.

Upgrades and Enhancements to Automated Passport Systems Are Behind Schedule

Automation upgrades and enhancements are the cornerstone of State's strategy to reduce the vulnerability of passport systems to fraud. Planned efforts involve (1) installing a computer network to connect all domestic passport agencies and serve as a platform to allow State to verify the multiple issuance of passports, (2) enhancing its travel document issuance system so that the passport photo can be printed digitally, and (3) completing the upgrade of its travel document issuance system at all passport agencies. State had planned to have most of the improvements completed by December 1995. However, only one major improvement, installation of a wide-area network, had been completed by that date. The other improvements, in addition to being dependent on the wide-area network for telecommunications, are also dependent on the completion of the upgrades to the passport production system. State's current goal is for full completion of these enhancements and upgrades by the end of 1996. State indicated that completion of these upgrades was dependent upon the availability of funds.

State installed the wide-area network to connect the passport agencies with each other as the telecommunications platform for the photo digitization and the multiple issuance verification initiatives. The Multiple Issuance Verification system is expected to allow Passport Office employees to detect individuals applying at more that one office for multiple passports using the same identity—which State describes as one of the most prevalent forms of passport fraud. Without such a system, there is no way for one office to know before issuance what applications are being processed by any other office. State is also developing a system to print a digitized passport photograph. According to State, a digitized photograph will make it easier to detect a substitution—another prevalent form of passport fraud. State spent about $4.1 million for these improvements in fiscal year 1995 and plans to spend an additional $22 million through fiscal year 1998. State is using revenues from the machine-readable visa processing fees to fund these improvements.

State has not completed the upgrade from the 1980 to the 1990 version of its Travel Document Issuance System, which is used to enter data, process, and track the actual production of passports. Systems in 9 of the 14 passport facilities have been upgraded. According to the Consular Bureau, the upgrade replaces an outdated minicomputer-based system with a more modern personal computer-based system, providing the interface needed to take advantage of the wide-area network and other new technologies. The conversion costs about $700,000 to $800,000 per office. Because of the high cost of the upgrade, the conversion had been proceeding at the rate of one passport agency per year. The Bureau used appropriated funds.

Conversion from the 1980 version to the 1990 version of the system is a prerequisite to implementing photo digitization and the Multiple Issuance Verification System. Therefore, the Consular Bureau plans to use machine-readable visa funds to pay for the conversion of the remaining five passport facilities. At those offices, the upgrades will be coupled with the installation of the photo digitization and the multiple issuance enhancements, which the Bureau believes will reduce costs. According to a Bureau official, depending on the availability of the funds, the Bureau plans to have all systems upgraded and enhanced by the end of calendar year 1996. However, the Bureau official acknowledged that this was an ambitious goal. He said variables such as the outcome of systems tests and the possibility that three of the passport offices may move could result in delays. Table 1 shows selected activities and corresponding milestone dates.

Table 1: Planned Improvements and Selected Milestone Dates

Activity	Original completion date	Actual or revised completion date
Upgrade Travel Document Issuance System at all agencies	No firm date established	December 1996
Install Wide-Area Network at all locations	March 1995	May 1995
Develop software for Multiple Issuance Verification System	December 1994	December 1995
Test Multiple Issuance Verification System process and procedures	March 1995	December 1996
Implement Multiple Issuance Verification System at all passport agencies	April 1995	December 1996
Test photo digitization at one agency	September 1994	December 1996
Install photo digitization hardware at all agencies	June 1995	December 1996

Agency Comments

In commenting orally on a draft of this report, State Department officials generally agreed with the report's presentation; however, they asserted that many of the generic problems listed in the report are the result of inadequate staffing and resources. They also noted that some points needed clarification or correction. We have incorporated these changes where appropriate.

Scope and Methodology

We conducted our review in Washington, D.C.; Canberra and Sydney, Australia; London, England; Guatemala City, Guatemala; Tokyo, Japan; Nairobi, Kenya; Seoul, Korea; Mexico City, Mexico; and Johannesburg, South Africa. We selected these posts to obtain a cross-section of large and small posts, posts with the machine-readable system, posts with the old visa-issuing system, and posts undergoing changes in their consular workloads.

We obtained past State Department Inspector General reports, annual Financial Management Integrity Act reports, and other documents describing visa and passport operations; reviewed agency plans for correcting the previously identified weaknesses; and discussed the status of the corrections with Bureau of Consular Affairs officials. We observed operations at the Washington Passport Agency in Washington, D.C., and at the overseas posts we visited we observed visa and passport operations, examined passport and visa applications, and tested selected internal control procedures.

We conducted our review intermittently from May 1994 to March 1996 in accordance with generally accepted government auditing standards.

Copies of the report are being sent to the Secretary of State, the Director of the Office of Management and Budget, and interested congressional committees. We will also provide copies to others upon request.

Please contact me at (202) 512-4128 if you or your staff have any questions concerning this report. Other major contributors are listed in appendix I.

Sincerely yours,

Jess T. Ford

Jess T. Ford, Associate Director
International Relations and Trade

Major Contributors to This Report

National Security and International Affairs Division, Washington, D.C.

Diana M. Glod
Jose M. Pena, III
Michael D. Rohrback
Cherie M. Starck
La Verne G. Tharpes
Steven K. Westley
Michael C. Zola

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON ♻ RECYCLED PAPER