GAO

For Release
on Delivery
Expected at
9:30 a.m. EDT
Tuesday,
May 20, 1997

STATE DEPARTMENT

Efforts to Reduce Visa Fraud

Statement of Benjamin F. Nelson, Director,
International Relations and Trade Issues,
National Security and International Affairs Division

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our 1996 report[1] on the Department of State's progress in making its visa issuance process more efficient and less vulnerable to fraud. The State Department is responsible for the issuance and integrity of the U.S. passport and visa, the world's most sought-after identity documents. State's visa issuance process is the first line of defense against fraudulent entry into the United States.

Summary

At the time of our review, State's strategy for reducing the potential for visa fraud was to (1) issue visas that are machine readable, (2) expand automated name-check capability to all posts, (3) form so-called "lookout" committees to identify suspected terrorists and others ineligible for visas, and (4) strengthen compliance with management controls. In May 1996, we issued a report assessing State's progress on these key initiatives based on our work at the State Department and nine overseas posts.[2]

In summary, we found mixed results. While the automation initiative had progressed after some delay, operational problems at some locations diminished the effectiveness of these efforts. These include

- technical problems that limited the availability and usefulness of the automated data base,
- inadequate cooperation by some key U.S. agencies in State's lookout committees, and
- lack of compliance with management control procedures.

While State has continued to move forward in automating its visa-issuance process, a recent report by State's Inspector General concluded that many problems still exist.

Nature of the Threat

As this Subcommittee is well aware, illegal immigration is a growing and complex problem. The Immigration and Naturalization Service (INS) estimates that as of October 1996, 5 million illegal aliens were residing in the United States. INS estimates that this number is increasing by about 275,000 persons annually. While not the primary source of illegal

---

[1]Passports and Visas: Status of Efforts to Reduce Fraud (GAO/NSIAD-96-99, May 9, 1996).

[2]The nine posts are Canberra and Sydney, Australia; London, England; Guatemala City, Guatemala; Tokyo, Japan; Nairobi, Kenya; Seoul, Republic of Korea; Mexico City, Mexico; and Johannesburg, South Africa.

GAO/T-NSIAD-97-167

immigration into the United States, visa fraud is a matter of concern. Illegal aliens are creative in their use of fraudulent documents to gain entry into the United States. A common practice is to paste the photo of an ineligible individual into a stolen passport with a valid visa or otherwise alter the data on the visa. Criminal passport and visa fraud arrests by State's Bureau of Diplomatic Security have more than doubled from 256 in 1992 to 567 in 1996.

State's Role

Controlling immigration to the United States is primarily INS' responsibility. State helps INS by issuing visas to citizens of other countries who want to visit the United States and identifying persons who should be excluded. Issuance of a visa, however, does not guarantee that the holder will be permitted to enter the United States. Rather, it permits the holder to apply at a port of entry. Responsibility for granting entry rests with the INS officer who conducts the inspection at the port of entry. In fiscal year 1996, State processed nearly 8 million nonimmigrant visa applications at over 200 visa-issuing posts. Thus, it is important that State's system work as efficiently and effectively as possible.

Weaknesses in State's Processes

Since 1987, State has recognized the lack of adequate controls over visa processing as a material weakness and an area of high risk.[3] State's Office of Inspector General has also identified a number of problems with visa operations. In response to these weaknesses and concerns about the growing problem of illegal immigration, State, beginning in 1989, developed a strategy to reduce the vulnerability of its processes to fraud. This strategy included improving and expanding automated systems and establishing embassy committees to identify individuals ineligible for visas. Full implementation of the machine-readable program was the primary initiative for eliminating visa fraud. State's plan also called for providing all visa-issuing posts with automated access to its global data base containing names of individuals ineligible for a visa. Later, State established embassy lookout committees designed to promote closer cooperation with other agencies in identifying individuals ineligible for visas. These efforts were to be combined with a greater emphasis on enforcement of internal management controls.

---

[3]Annual reports are required by the Federal Managers' Financial Integrity Act.

Technical Problems Reduce Effectiveness of Visa Automation

In 1989, State began the machine-readable visa program as its primary initiative for eliminating the use of 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, INS and the U.S. Customs Service can check names by scanning the machine-readable zone of the visa. The visas also include a photograph of the traveler.

The machine-readable visa, in conjunction with expanded access to the automated lookout system, can significantly reduce the vulnerability of the system to fraud. State originally intended to have the machine-readable visa system installed by 1991. However, the program suffered from delays and insufficient funds. In addition, automated access to the lookout system was not available at all posts. 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 that fiscal year. The Congress authorized State to retain machine-readable visa processing fees to fund these and other improvements.

At the time of our review, State had installed the machine-readable visa system at 200 posts. In addition, all of the posts had automated access to the Consular Lookout and Support System (CLASS) either through direct telecommunications lines to the CLASS data base in Beltsville, Maryland, or via the distributed name check (DNC) system, a stand-alone personal computer system with the CLASS data base on tape or compact disk.

In April 1997, State testified that (1) every visa-issuing post has the machine-readable visa system installed, and had direct access to CLASS; and (2) it had developed and is now installing a new version of the machine-readable system, called MRV-2, at all visa-issuing posts. State spent about $12.9 million on installation of the MRV-2 in fiscal year 1996, plans to spend $24 million in fiscal year 1997, and has requested $32 million for fiscal year 1998.

Although most posts had automated name-check capability and machine-readable visa systems at the time of our review, technical problems limited their usefulness and availability. Posts often experienced transmission problems with the telecommunications lines that support the

system. U.S. missions in Mexico City, Guatemala City, Sydney, Nairobi, and Seoul experienced problems with the telecommunications lines and interruptions of CLASS. These disruptions 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 doing so, 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 the microfiche list.

State's Diplomatic Telecommunications Service Program Office works with international telecommunications carriers to find solutions where possible. However, if the problem is in the telecommunications lines of the host country, little can be done except to improve the post's backup system.

Lack of Cooperation Limits Usefulness of Lookout Committees

Effective efforts to limit visa fraud call for the skills, resources, and coordination of many U.S. government agencies. 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 the consulates in Sydney and Johannesburg had 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. A number of agency representatives were 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. They attributed their reluctance 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 were represented on these committees. For

example, according to a consular official, the committee in Pretoria did not include representatives from the Federal Bureau of Investigations, the Customs Service, and the Drug Enforcement Agency. The committee in Tokyo also lacked key representatives.

Consular officials told us 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. We have not assessed the effectiveness or extent of these headquarters' initiatives.

Overseas Posts Do Not Always Adhere to Internal Controls

Maintaining the integrity of the process requires that posts adhere to established controls. This was not always the case. One common shortcoming we observed was the use of foreign service nationals (FSN) to check names through CLASS without the direct supervision of a U.S. officer. FSNs were responsible for checking names at five of the posts we visited. The consular officers at these posts relied on FSNs to notify them when an applicant's name matched one in the CLASS data base. At the time of our review, three of the posts also were not equipped with the machine-readable visa system, which automatically provides the results of the name check for the U.S. officer's review. Officials of State's Bureau of Consular Affairs told us that the machine-readable system has since been installed at these locations and improved procedures and software enhancements now make unsupervised name checks impossible. Consular officers are now required to certify in writing that they have checked the automated lookout system and that there is no basis for excluding the applicant. We have not assessed the extent or the effectiveness of compliance with this new requirement.

Other internal control shortcomings were the lack of security over controlled equipment and supplies and the failure to report and reconcile daily activities and follow cashiering procedures. Bureau of Consular Affairs officials attributed some of these problems to a lack of resources.

Inspector General Reports That Some Problems Remain

In May 1997, State's Office of Inspector General issued a report that concluded that some of the problems with the machine-readable visa program still exist. The Inspector General reported that some posts are still having difficulties accessing CLASS as a result of interruptions to telecommunications lines or the mainframe computer. Further, the Inspector General identified significant software limitations with the DNC that may prevent posts from having full information at the time of visa adjudication. The report stated that the Bureau of Consular Affairs has developed and distributed a newer version of the DNC that will address these limitations.

The Inspector General further reported that, although all posts now have the machine-readable visa system, the border security and inspection process remains vulnerable with respect to validating a visa. There is no automated mechanism for transmitting data about nonimmigrant visa issuance to ports of entry to determine whether the machine-readable visa being presented for entry into the United Sates is a valid visa issued by the Department. Moreover, INS is not reading the encryption code to authenticate the visa. According to State, the new machine-readable visa will have the capability to electronically transmit relevant nonimmigrant visa data to ports of entry. The Inspector General also reported that management and accountability over machine-readable visa supplies and equipment continues to be a problem.

The report attributed some of the problems to severe staffing shortages and the Bureau of Consular Affairs' failure to address software and hardware problems early in the development of the machine-readable visa program. While recognizing that the new version of the machine-readable visa is designed to correct some of the shortcomings, the Inspector General made a number of recommendations to address other weaknesses in the process.

Conclusion

In closing, the State Department has made progress in automating and modernizing its visa-issuance process to reduce its vulnerability to fraud. However, improvements are still needed to better protect the integrity of U.S. entry documents.

This concludes my prepared remarks, Mr. Chairman and Members of the Subcommittee.

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested