U.S. Senate Homeland Security and Government Affairs Committee

Hearing on GAO Report 05-477,
"Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts"

Testimony of Frank E. Moss
Deputy Assistant Secretary for Passport Services
Bureau of Consular Affairs
U.S. Department of State

June 29, 2005

Chairman Collins, Ranking Member Lieberman, Distinguished Members of the Committee:

I am pleased to be here today to discuss what the State Department is doing to respond to the concerns raised by the Government Accountability Office in its Report entitled "Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts." I want to thank the GAO and especially their lead examiner, Michael Courts, for their hard work on this project. As the GAO report recognizes, the Department of State is already engaged in many areas to protect the integrity of the U.S. passport, working hand-in-hand with the State Department's Diplomatic Security Service, and with elements of the Homeland Security and Justice Departments. Still, we acknowledge that it is always possible to improve, and welcome GAO's observations and suggestions.

The integrity of the passport rests upon three major elements: the quality of the adjudication process, the security features of the passport itself, and the introduction of biometrics to make certain that the passport can only be used by the person to whom it is issued. Taken together, these elements constitute a comprehensive approach to passport security. Securing the document and the adjudication process is particularly important in an era when terrorists, transnational criminals and others seeking to enter the U.S. illegally view travel documents as valuable tools. By making sure that U.S. passports are only issued to American citizens, that they are more difficult to counterfeit and that the bearer of the passport is the same person

to whom the passport was issued, the Department of State actively enhances the security of this nation, while we continue to promote our international engagement through personal, commercial, educational and research exchanges with other nations.

During the last fiscal year the Department of State processed a total of 8.8 million U.S. passport applications. This set a record, exceeding the total from the previous year by more than one million applications and representing a workload increase of some 22 percent. This year, the Department of State is experiencing a 14 percent rise. So far in FY-2005, the Department has already processed more than 7 million passport applications and we are on track to adjudicate more than 10 million passports by the end of the fiscal year. This means that overall passport demand will have increased by approximately 40 percent in just two years.

As the Department of State develops plans to address the increase in demand for U.S. passports resulting from normal growth in international travel, their use by Americans, especially recently naturalized citizens, as portable proof of identity and nationality, and the Western Hemisphere Travel Initiative, we are dedicated to actively pursuing initiatives to improve the integrity of the U.S. passport. I would like to give you an overview today of what we have done and are doing to improve passport integrity.

Strengthening the Adjudication Process

A key objective is to ensure that U.S. passports are issued only to persons who are entitled to them. This process begins with a careful examination of identity and citizenship documentation, especially birth and naturalization certificates. Increased information sharing, both within the United States Government and with its partners overseas, is one of the most effective ways to strengthen this process so that only those entitled to U.S. citizenship receive a U.S. passport. This is a critical element in our strategy to "look behind the paper" in terms of passport adjudication.

The Department of State has actively worked to establish data exchange programs with other Federal agencies, as well as organizations like INTERPOL, in a manner that is mutually beneficial and that will keep U.S. passports out of the hands of those who are not eligible to receive them. For example, in April 2004, the Department signed a memorandum of understanding with the Social Security Administration (SSA) that would

permit the Department to verify the Social Security numbers of U.S. passport applicants. This measure provides another verification tool for passport specialists and consular officials adjudicating passport applications by allowing them to correlate the data provided by a passport applicant with information in SSA's system and use this information to support decisions about an applicant's identity. This initiative has now "gone live" at our passport agency here in Washington and will be operational nationwide by early August.

The Department has a long-standing and effective working relationship with federal law enforcement agencies that targets passport applicants of particular concern. Today, we have nearly 50,000 names of fugitives or other individuals of interest to law enforcement in the passport lookout system. Half of these were entered individually as a result of our outreach efforts. The other half of these entries are based on U.S. Marshals Service (USMS) federal fugitive warrants, data that the Department took the initiative to obtain.

To complement the USMS information, work is well underway to add to the passport lookout system an extract of FBI fugitive warrants from the NCIC Wanted Persons File. I am glad to report that last week we received a letter from the FBI that responds positively to our request for access to information on an additional group of persons subject to federal warrants who are sought by other federal law enforcement agencies. In addition, this positive response from the FBI may also open the door to access comprehensive information on persons subject to state and local warrants. Right now, we rely on the voluntary information exchange with law enforcement officials at the state and local levels which we have promoted through the sending of a letter from the Assistant Secretary of State for Consular Affairs to all the states' attorneys general. Having access to NCIC data would be far more desirable.

In 2004, the Department reached an agreement with INTERPOL to provide the Department's lost and stolen passport database to that organization via the U.S. National Central Bureau (NCB). The NCB shares the data with INTERPOL, which in turn makes this information available to all INTERPOL member states. The U.S. lost and stolen passport database currently contains the passport numbers of over 661,000 U.S. passports, that is, nearly 10 percent of the INTERPOL database. It is important to note that once a U.S. passport is reported lost or stolen, it is no longer valid for travel.

The Department of State is about to sign an agreement with the Terrorist Screening Center (TSC) that will provide information on American citizens who are of concern to TSC due to a nexus to terrorism or an ongoing investigation. This datashare program will enable the Terrorist Screening Center to learn of the passport application of an individual of interest and, under appropriate circumstances, take law enforcement action.

In addition, the Department of State provides to the National Counter Terrorism Center (NCTC) access to the Passport Records Imaging System Management (PRISM). This database includes scanned images of all passport applications since 1994.

Maintaining an aggressive fraud prevention program is another important element in safeguarding the adjudication process. The Department of State has undertaken a comprehensive review of its fraud prevention efforts and implemented a number of initiatives, including organizational improvements, enhanced training, regulatory changes, new tools, and new programmatic activities with domestic and international partners. All senior passport specialists now rotate through the fraud prevention office at domestic passport facilities to give them specialized experience in fraud detection. We see this effort as being crucial in helping to ensure that the specialized information and knowledge available in the Fraud Prevention Program office is available to passport specialists. Let me be clear—it is passport examiners who serve as the first line of defense against passport fraud. We are committed to giving them and their supervisors all appropriate tools to help them fulfill that responsibility. We see this rotational program as a key element in that effort.

The "lessons learned" from fraud investigations also directly influences our regulatory practices. To help prevent international child abduction, we now require that both parents consent to the issuance of a passport for a child. We also now mandate the presence of children under the age of 14 when passport applications are executed on their behalf. We are also making greater use, with the appropriate respect for privacy concerns, of commercial databases to assure that persons applying for passports are who they claim to be. Finally, we are conducting unannounced audits of passport agencies to review applications for proper adjudication, consistency and attention to fraud indicators. Results of these unannounced audits suggest to me that our anti-fraud strategy is effective; based on results

from eight agencies, we have a rate of about 1.76 percent in which non-serious errors were made by passport specialists in documenting passport applications. This is, of course, an opportunity for retraining our staff. The rate of potentially serious frauds identified through this validation study is far lower, running based on our preliminary results at about 3 per 10,000 passport applications.

The focus on fraud prevention is already paying dividends. Statistics for this fiscal year show an increase in referrals to fraud prevention offices, as well as an increase in the referral of presumptive fraud cases to the Department's Bureau of Diplomatic Security (DS) for further investigation. The Bureau of Consular Affairs enjoys excellent cooperation and support from DS, which has the responsibility for criminal investigations involving passport fraud. The statistics about the efficacy of joint Consular Affairs-Diplomatic Security efforts are compelling. So far in fiscal year 2005, DS opened 2,401 passport investigations and made 375 arrests; this represents a significant increase over the same period in 2004, when DS opened 1,722 cases and made 183 arrests.

Strengthening The Security of the Passport

Efforts to strengthen the adjudication process and augment fraud prevention efforts would be less effective if we did not attend to the other key elements of passport security with equal fervor. Turning to the passport itself, the Department recently completed the first cover-to-cover redesign of the document in more than a decade. The new passport includes a host of new security features, including sophisticated new fraud-resistant artwork, adopting printing techniques used in the current generation of U.S. currency, and other changes that significantly increase the physical security of the U.S. passport.

Our objective in designing the new passport is to further raise the bar against counterfeiting or the fraudulent use of lost or stolen passports. Advances including color shifting ink, microprinting, latent image lettering and a security laminate over the biographic data page that includes optical variations, all serve to deter counterfeiters and forgers. The biographic data page is being relocated from the inside of the front cover to the first inside page for added security. The inventory control number for each book is now the same as the passport number. Imagery on the inside pages of the passport incorporates more colors, stylized depictions of iconic American

scenes, and includes famous quotations from American history. The new passport, combined with security enhancements in the adjudication process, helps to ensure that only qualified applicants receive U.S. passports.

I am happy to share with the members of the Committee samples of the new passport.

Strengthening Passport Integrity Through Use of Biometrics

This next generation of U.S. passport, the e-passport, includes biometric technology that will further support the Government's border security goals. Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the Department of State issued that passport.

Consistent with globally interoperable biometric specifications adopted by the International Civil Aviation Organization (ICAO) in May 2003, the United States has adopted the facial image as the first generation of biometric identifiers. The new U.S. passport includes a contactless chip in the rear cover of the passport that will contain the same data as that found on the biographic data page of the passport, including a digital image of the bearer's photograph. This data includes the following information about the bearer: the photograph, the name, the date and place of birth, as well as the passport number and the date of issuance and expiration all of which is protected by a unique encrypted signature. Looking to the future, the Department decided to require 64 KB of writeable memory on the contactless chip in the event that we subsequently decide to introduce additional biometrics. Should the United States Government decide to change the biometric requirements, this change will be subject to vetting through the Federal Register process.

On June 15, the Department, partnering with the Department of Homeland Security and in collaboration with Australia and New Zealand, launched an operational field test to measure the overall performance of the e-passport, issuing approximately 250 U.S. e-passports to personnel employed by United Air Lines and who fly internationally to or from Los Angeles. The Department of Homeland Security has developed separate lanes and installed e-passport readers to test their efficiency. Later this year, we will expand this pilot program to include diplomatic and official passports, with national deployment of the e-passport scheduled for 2006.

The Department of State is well aware of concerns that data written to the contactless chip in the e-passport may be susceptible to unauthorized reading. To help reduce this risk, anti-skimming materials that prevent the chip from being read when the passport book is closed or mostly closed will be placed in the passport.

The Department is confident that the new e-passport, including biometrics and other improvements, will take security and travel facilitation to a new level. Naturally, the Department will comprehensively test the operation and durability of the e-passport and work to resolve any issues as they occur. In fact, the Department of State is engaged in a continuous product improvement effort with regard to the U.S. passport. We will continue to monitor technical developments and help conduct research to ensure that we produce a passport that is highly secure, tamper resistant and globally interoperable.

The GAO's Recommendations

As I mentioned above, the passport name clearance system contains over 50,000 entries of persons wanted at the Federal, state and local levels. We agree with the GAO that enhanced interagency datasharing can improve that system significantly. Some of the need can be met almost immediately, while other aspects will require systems and program development. But we are well on the way to filling a gap in the system. As I said earlier, we are in the final stages of completing an MOU with the Terrorist Screening Center that will result in their U.S. Persons database being added to the Passport name check system.

GAO recommends the development and deployment of a national fraud library of suspect documents to allow our staff nationwide to efficiently access and share fraud prevention information and tools. Presently, there are several different resources that provide such information and we agree that finding a way to bring them together is desirable. An option we are pursuing in this regard is the U.S. Secret Service's (USSS) Questionable ID Documents (QID) database, which includes a section on valid documents, one on stolen documents and another on counterfeits and alterations. We are working with the Secret Service to obtain access to this database. An advantage of this system is the fact that we can contribute to

their database, and in doing so, assist them in their mission, while also avoiding significant development costs. We are also working to obtain electronic authentication of driver's licenses while also allowing the states access to passport data to help them verify the identity of their applicants.

The GAO recommends designating additional positions for fraud prevention coordination and training in domestic passport issuing offices, and establishing a more formalized fraud prevention training regimen. We agree, and have taken several steps to make this a reality. We are in the process of adding more Fraud Prevention Managers to the staffs of our larger agencies, and we have increased the numbers of persons working in the fraud offices, as well as the length of time they spend there. This will have a direct impact on improving the training that is provided to the Passport Specialists who adjudicate passport applications. Finally, under a Headquarters reorganization nearing completion, we are adding to the staff that coordinates and backstops the Fraud Prevention operations in the field agencies. Part of the work of the expanded Headquarters staff will be to develop a national fraud training program for the Specialists.

GAO looked at the issue of workload transfers from one domestic agency to another, which we do to make the best use of our issuance capabilities system-wide and because most of our work flows through a fee depository process. A theoretical risk in having applications from one region of the country adjudicated in another is missed opportunities to identify fraud because of a lack of familiarity with citizenship evidence from the originating region. We believe that we successfully address this risk through our selection of highly skilled Fraud Program managers, by rotating our senior passports specialists through the FPM office so that they can then assist and better train their staff, and by training centrally all of our newly hired specialists.

Finally, the GAO suggested increasing training and oversight of the 7,000-plus passport application acceptance agents nationwide, principally Postal Service employees and clerks of court, which perform the valuable service of accepting applications from U.S. citizens and in doing so bring the passport application process to the our citizens. In addition to being our representatives, they are the first line of defense in that they identify the passport applicant as the person he or she claims to be. Improved training is already underway through use of Computer Based Training (CBT) modules that have been developed in cooperation with the US Postal Service. Those

modules are also being adapted for use by other facilities. There are also initiatives in process to more closely monitor the quality of the work received from the acceptance agents.

Madam Chairman, I am grateful for the opportunity today to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. Again, we appreciate GAO's constructive recommendations and look forward to working with Congress and the GAO to produce the most secure passport possible. At this time, I am happy to answer any questions you, the Ranking Member and the other distinguished members of the Subcommittee might have about the Department's fraud prevention efforts or the other facets of the U.S. passport program that I have discussed.