

GAO

Testimony

Before the Subcommittee on Terrorism
and Homeland Security, Committee on the
Judiciary, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Tuesday, May 5, 2009

STATE DEPARTMENT

**Significant Vulnerabilities in
the Passport Issuance
Process**

Statement of Jess T. Ford, Director
International Affairs and Trade



GAO

Accountability * Integrity * Reliability

May 5, 2009

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our recent work on significant fraud vulnerabilities in the passport issuance process. My testimony today will highlight the results of our March 2009 report on undercover investigative tests, which confirmed the continued existence of significant fraud vulnerabilities in this process.¹ We also provided a letter to you in April 2009, describing our recent work on passport fraud and summarizing actions the Department of State (State) has taken to address the prior weaknesses related to fraud vulnerabilities we identified.² We have found that these vulnerabilities stem from people, process, and technology. For example, the lack of training and resources provided to people contributes to vulnerabilities in the detection of fraudulent applications and counterfeit documents. The limitations in the access to inter-agency information contribute to vulnerabilities related to processes. Finally, the lack of databases and information-sharing technologies contribute to vulnerabilities in the verification of passport applicants' records. I will also discuss the status of prior recommendations and suggested corrective actions we have made to reduce fraud risk in the passport program.

A U.S. passport not only allows an individual to travel freely in and out of the United States, but also can be used to obtain further identification documents, prove U.S. citizenship, and set up bank accounts, among other things. Because passports issued under a false identity help enable individuals to conceal their movements and activities, there is great concern that passport fraud could facilitate acts of terrorism. Further, passport fraud facilitates other crimes such as illegal immigration, money laundering, drug trafficking, tax evasion, and alien smuggling. Malicious individuals may seek to exploit vulnerabilities in State's current passport issuance process, such as a lack of due diligence on the part of examiners who screen applications, by using counterfeit or fraudulently obtained

¹See GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, [GAO-09-447](#) (Washington, D.C.: Mar. 13, 2009).

²See GAO, *Addressing Significant Vulnerabilities in the Department of State's Passport Issuance Process*, [GAO-09-583R](#) (Washington, D.C.: April 13, 2009).

documents as proof of identity and U.S. citizenship to obtain genuine U.S. passports.³

My comments today are based on our previously issued reports, which we performed in accordance with standards set forth by the Council of Inspectors General for Integrity and Efficiency (CIGIE) and generally accepted government auditing standards.

Undercover Investigation Confirms Continued Existence of Significant Fraud Vulnerabilities in the Passport Issuance Process

In March 2009 we reported on the results of our investigation into the vulnerabilities of State's passport issuance process. Specifically, we reported our undercover investigator was easily able to obtain four genuine U.S. passports using counterfeit or fraudulently obtained documents. For this investigation, we designed four test scenarios that would simulate the actions of a malicious individual who had access to another person's identity information (a practice commonly known as identity theft). We then attempted to obtain four genuine U.S. passports by using counterfeit or fraudulently obtained documents, such as birth certificates and drivers' licenses, and the Social Security Numbers (SSN) of fictitious or deceased individuals. In the most egregious case, our investigator obtained a U.S. passport using counterfeit documents and the SSN of a man who died in 1965. In another case, our undercover investigator obtained a U.S. passport using counterfeit documents and the genuine SSN of a fictitious 5-year-old child—even though his counterfeit documents and application indicated he was 53 years old.

The results of our investigation confirmed that State continues to struggle with reducing fraud risks we have previously identified at both the application point and the adjudication point⁴. In 2005, we reported weaknesses in State's information sharing with federal and state agencies.⁵

³As required by State's instructions on the Application for a U.S. Passport, form DS-11, applicants must provide proof of U.S. citizenship and proof of identity, along with two recent color photographs and funds to cover the passport application fees.

⁴Through a process called adjudication, passport examiners determine whether they should issue each applicant a passport. Adjudication requires the examiner to scrutinize identification and citizenship documents presented by applicants to verify their identity and U.S. citizenship. It also includes the examination of an application to detect potential indicators of passport fraud and the comparison of the applicant's information against databases that help identify individuals who may not qualify for a U.S. passport.

⁵See GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, [GAO-05-477](#) (Washington, D.C.: May 20, 2005).

For example, we reported that State did not receive information on U.S. citizens listed in the federal government's consolidated terrorist watch list and State does not routinely obtain the names of other individuals wanted by both federal and state law enforcement authorities. We also found that the information that State received from the Social Security Administration (SSA) was limited and did not include access to SSA's death records, although State officials said they were exploring the possibility of obtaining these records in the future. A little over 2 years later, in July 2007, we reported that many previously identified problems in the oversight of the acceptance facilities⁶ persisted and noted that State lacked a formal oversight program for its acceptance facilities to ensure effective controls are established and monitored regularly.⁷ We concluded more needed to be done because of the critical role acceptance agents play in establishing the identity of passport applicants, which is critical to preventing the issuance of genuine passports to criminals or terrorists as a result of receipt of a fraudulent application.

State Indicated It Is Taking Actions to Address GAO Reports

With regard to adjudication, State officials told us a lack of access to information contributed to the failures identified by our recent undercover tests. According to State, passport specialists did not wait for the results of a required SSA database check before approving our fraudulent applications. In all four of our tests, State failed to identify the fraudulent birth certificates we used. State officials attributed these failures to a lack of access to state-level vital records data that would have allowed passport specialists to verify the authenticity of the birth certificates. State officials indicated they were exploring ways to access vital records and department of motor vehicle records nationwide to address the lack-of-access issues. In the case of our most egregious application—in which we fraudulently obtained a passport using the SSN of a man who died in 1965—State officials said that the lack of an automated check against SSA death records has been a long-standing vulnerability of the passport adjudication process. In an attempt to provide automatic death record information for

⁶Passport acceptance facilities are located at certain U.S. post offices, courthouses, and other institutions and do not employ State Department personnel. The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document (such as a driver's license) actually matches that applicant.

⁷ See 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).

all cases reviewed during adjudication, Passport Services officials represented that they have recently purchased a subscription to the *Death Master File* which includes weekly updates of deaths recorded by SSA. Passport Services intends for the *Death Master File* check to supplement the other checks in the adjudication process and not replace the current returns from SSA. Further, we note that State issues passports to some individuals who do not provide SSNs, meaning that State cannot rely on an SSN check to identify all fraudulent applications.⁸

With respect to the acceptance process, State officials told us that they are working toward improving oversight of passport acceptance facilities as we recommended in our July 2007 report. In that report we recommended that State establish a comprehensive oversight program for passport acceptance facilities. In September 2008, Passport Services announced the establishment of an Acceptance Facility Oversight Program within the Office of Passport Integrity and Internal Controls. According to State, the oversight program will include audits, monitoring, and reporting on each acceptance facility's adherence to Passport Service's national policies and procedures, and to make recommendations for corrective actions for any deficiencies identified throughout the application process. State plans to implement the program in phases from 2009 to 2013.

In addition, State officials also told us that they took several actions in direct response to our undercover investigation. State suspended the adjudication authority of the passport specialists responsible for approving our fraudulent applications and the authority of the facilities that accepted our applications pending additional antifraud training. It revised the performance standards for passport specialists to eliminate the production targets for 2009, while all other aspects of performance standards were left intact for quality and fraud prevention purposes. State officials added that Passport Services will be conducting a study and working with the union to develop new production targets. These targets will not be in place until 2010. State identified additional tools and systems that would help address vulnerabilities within the issuance process.

⁸According to State, between June 20, 2008, and December 22, 2008, a total of 71,982 applicants received passports without supplying their SSN.

Prior Recommendations and Corrective Actions

Since 2005 we have made several recommendations to State to improve the coordination and execution of passport fraud detection efforts, including considering ways to improve interagency information sharing and strengthening fraud prevention training. We also recommended that State consider conducting performance audits of acceptance facilities, agents, and accepted applications. State generally concurred with our recommendations and implemented many of them.

Nonetheless, our recent investigation shows that serious vulnerabilities remain. The Secretary of State should ensure that our prior recommendations are adequately addressed and that all currently planned corrective actions are successfully implemented. We also suggested that the Secretary of State take the following corrective actions:

- improve the training and resources available to passport acceptance facility employees for detecting passport fraud, especially related to detecting counterfeit documents;
- for applications containing an SSN, establish a process whereby passport specialists are not able to issue a passport prior to receiving and reviewing the results of SSN and *Death Master File* checks, except under specific or extenuating circumstances and after supervisory review;
- explore commercial options for performing real-time checks of the validity of SSNs and other information included in applications;
- conduct “red team” (covert) tests similar to our own and use the results of these tests to improve the performance of passport acceptance agents and passport specialists; and
- work with state-level officials to develop a strategy to gain access to the necessary state databases and incorporate reviews of these data into the adjudication process.

Conclusion

In conclusion, Mr. Chairman, State officials have known about vulnerabilities in the passport issuance process for many years but have failed to effectively address these vulnerabilities. Although State has proposed reasonable oversight measures for passport acceptance facilities in response to our prior recommendations, it is too early to determine whether these measures will be effective. Our most recent investigation reveals passport specialists also face challenges. State has indicated that it takes the results of this investigation very seriously, and officials have said that they are taking agencywide actions. Given the potential exploitation

of vulnerabilities in State's current passport issuance process by criminals and terrorists, State should take seriously its efforts to maintain the integrity of the passport issuance process to protect U.S. citizens and interests at home and abroad.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittee may have at this time.

For further information about this statement, please contact Jess Ford at (202) 512-4128 or fordj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

