



United States Government Accountability Office
Washington, DC 20548

April 13, 2009

The Honorable Jon Kyl
Ranking Member
Subcommittee on Terrorism and Homeland Security
Committee on the Judiciary
United States Senate

The Honorable Dianne Feinstein
United States Senate

Subject: *Addressing Significant Vulnerabilities in the Department of State's
Passport Issuance Process*

A genuine U.S. passport is a vital document, permitting its owner to travel freely into and out of the United States, prove U.S. citizenship, obtain further identification documents, and set up bank accounts, among other things. Since May 2005, we have issued several reports identifying significant fraud vulnerabilities in the passport issuance process.¹ This report (1) describes our recent work on passport fraud and (2) summarizes actions the Department of State (State) has indicated it is taking to address the fraud vulnerabilities we identified. We are also providing suggested corrective actions to reduce fraud risk in the passport program.

We met with State officials and reviewed relevant documentation in preparing this letter. We performed our work from March to April 2009 in accordance with standards set forth by the Council of Inspectors General for Integrity and Efficiency (CIGIE). We did not attempt to verify the statements of State officials.

¹GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, [GAO-05-477](#) (Washington, D.C.: May 20, 2005); *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); and *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, [GAO-09-447](#) (Washington, D.C.: Mar. 13, 2009).

Background

State operates 18 domestic passport-issuing offices or centers, where most passports are issued each year.² To obtain a passport, U.S. citizens may apply in person either at a domestic State-run facility or at one of over 9,000 passport acceptance facilities across the country. Passport acceptance facilities are located at certain United States Postal Service (USPS) locations, courthouses, and other institutions, and do not employ State 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 the applicant, and sending each applicant's proof of citizenship and passport application to State. The State employees who examine applications are called passport specialists.

Fraud risk. In 2005, we reported that using the stolen identities and documentation of U.S. citizens is the primary tactic of those fraudulently applying for U.S. passports, and that passport fraud is often linked to other crimes. Our report mentioned a number of ways in which a person might fraudulently obtain a U.S. passport, including using an assumed identity that is supported by genuine but fraudulently obtained identification documents; submitting false claims of lost, stolen, or mutilated passports; using counterfeit citizenship documents; and using the identity of a deceased person. We also reported weaknesses in State's information sharing with other federal agencies. For example, we stated that the information that State received and used from the Social Security Administration (SSA) was limited and outdated. We noted that although State and SSA signed a memorandum in April 2004 that gave State access to SSA's main database to help verify passport applicants' identity, the memorandum had not been implemented as of March 2005. Moreover, we reported that the memorandum did not include access to SSA's death records, but that State officials said they were exploring the possibility of obtaining these records in the future.³ We made several recommendations to State to improve the coordination and execution of passport fraud detection efforts, including recommendations to create an electronic library on fraud and to develop a core curriculum for passport examiners. State generally concurred with our recommendations and implemented the majority of them.

Passport acceptance facilities. A little over 2 years later, in July 2007, we recommended that State take additional actions to address weaknesses in the oversight of passport acceptance facilities (e.g., USPS locations). While we reported

²These offices are located in Aurora, Colorado; Boston; Charleston, South Carolina; Chicago; Detroit; Honolulu; Houston; Los Angeles; Miami; New Orleans; New York; Norwalk, Connecticut; Philadelphia; Portsmouth, New Hampshire; San Francisco; Seattle; and two sites in Washington, D.C.—a regional passport agency and a special issuance agency that handles official U.S. government and diplomatic passports. While most of these facilities are regional passport agencies that process in-person applications in addition to applications received by mail, the facilities in Charleston, South Carolina, and Portsmouth, New Hampshire, are megaprocessing centers with no public access. In addition, State has two passport personalization facilities located in Tucson, Arizona; and Hot Springs, Arkansas.

³On June 29, 2005, a State official testified before the Senate Committee on Homeland Security and Governmental Affairs that the initiative with SSA would be operational nationwide by early August 2005.

State had taken actions to address some weaknesses we had previously identified in the acceptance agent program, such as the need for improved training of acceptance agents, we found that many of the previously identified problems in the oversight of the acceptance facilities persisted. Specifically, State lacked a formal oversight program for its acceptance facilities to ensure effective controls are established and monitored regularly, a lack that State officials believed contributed to problems with applications received through acceptance agents. 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. To address these vulnerabilities, we recommended that State establish a comprehensive oversight program for passport acceptance facilities including an appropriate system of internal controls. We also recommended that State consider conducting performance audits of acceptance facilities, agents, and accepted applications. State agreed with these recommendations and indicated that it planned to implement them.

Undercover tests. In March 2009, we reported that our undercover tests confirmed the continued existence of significant fraud vulnerabilities in the passport issuance process. Our undercover investigator was easily able to obtain four genuine U.S. passports using counterfeit or fraudulently obtained documents. In the most egregious case, our investigator obtained a U.S. passport using counterfeit documents and the Social Security number (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. State and USPS employees did not identify our documents as counterfeit in any of our four tests. State officials agreed that our investigation exposed a major vulnerability in the department's passport issuance process and acknowledged that they have issued other fraudulently obtained passports in the past. In order to improve State's current passport fraud detection capabilities, officials said that State would need greater cooperation from other agencies at both the federal and state levels, and the ability to access other agencies' records in real time. State officials informed us that they revoked the four fraudulently obtained U.S. passports and that they would study the matter further to determine what steps would be appropriate to improve passport issuance procedures. We did not attempt to determine what checks, if any, State performed when approving our fraudulent applications. We did not make any recommendations as a result of this investigation.

State Indicated It Is Taking Actions to Address GAO Reports

State continues to struggle with reducing fraud risks at both the application point and the adjudication point. With respect to acceptance, State officials told us that they are in the process of improving oversight of passport acceptance facilities as we recommended in our July 2007 report. For example, 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 make recommendations for corrective actions for any deficiencies identified throughout

the application process. State intends to develop practices and procedures to improve the safeguarding of applicants' personal information, and develop standardized national policies and procedures to deactivate noncompliant acceptance facilities. State has identified additional resources to support the development of the program, including funding, staffing, and the development of database systems to track the performance of acceptance facilities. State plans to implement the program in phases from 2009 to 2013, and expects the initial phase of the program to be completed by summer 2009; it will include hiring 44 program staff, developing a training curriculum for staff conducting audits, and identifying vulnerabilities.

Regarding adjudication, State officials told us that a combination of human error and a lack of access to information resulted in the failures identified by our 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. 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.⁴

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 all cases reviewed during adjudication, Passport Services represented that it has 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.

State officials also told us that they took several actions in direct response to our undercover investigation, including the following:

- State suspended the adjudication authority of the four passport specialists responsible for approving our fraudulent applications pending additional training. It is auditing all work completed by these specialists.
- State suspended the authority to accept passport applications at the USPS facilities that accepted our applications pending additional antifraud training.

⁴According to State, between June 20, 2008, and December 22, 2008, a total of 71,982 applicants received passports without supplying their SSN.

- State revised performance standards for passport specialists to eliminate the production targets for 2009. In addition, State implemented a temporary requirement that supervisors review all adjudicated applications prior to approval.⁵ All other aspects of performance standards were left intact for quality and fraud prevention purposes.
- State identified additional tools and systems that would help address vulnerabilities within the issuance process.

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.

Conclusions

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 July 2007 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 seriously, and officials have said that they are taking agencywide actions. The fact that our undercover investigator obtained a genuine U.S. passport using the SSN of a man who died in 1965 is particularly troubling given that a simple check of SSA's publicly available *Death Master File* would have disclosed the fraud.

Corrective Actions

The Secretary of State should ensure that all currently planned corrective actions are successfully implemented and that our prior recommendations are adequately addressed. Further, we suggest that the Secretary of State take the five 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;

⁵State initiated the temporary requirement for supervisory reviews on March 2, 2009. According to one high-level State official, State implemented the required review for all passport specialists agencywide for a period of 8 business days, after which supervisors have begun gradually releasing passport specialists from the requirement at the discretion of their supervisors once supervisors deem the passport specialists' performance to be satisfactory. The reviews require supervisors to examine the same documentation and database information as the passport specialists, review application annotations, and then suspend, approve, or deny the applications. This temporary review requirement is scheduled to end on May 31, 2009.

- 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;

Agency Comments

State provided comments in response to a draft of this letter. State acknowledged all of our suggestions to help address vulnerabilities in the adjudication process and potential fraud risks. State also provided comments on additional actions it stated it had begun or planned to begin to further address vulnerabilities and potential fraud risks. For example, State noted it has established a working group to evaluate the entire adjudication program and determine ways to provide a more thorough adjudicative review of passport applications. State also noted that it plans to identify and target acceptance facilities in need of more training as part of its new oversight program and plans to provide acceptance facilities with additional guidance on identifying counterfeit documents. In addition, State noted that it currently uses commercial databases for some aspects of its adjudication process, and is considering building checks on these databases into the frontend of the process.

We acknowledge these are positive steps, but we believe State must follow through with these actions to effectively address the significant fraud vulnerabilities we identified. Moreover, State’s response to our comments raises questions about whether State has adequately implemented the antifraud measures it claims to now have in place. For example, State indicates in its comments that in October 2008, it “implemented technology that requires any application with a death match to be removed from regular processing and submitted to the fraud manager for additional review.” However, we received a genuine U.S. passport using the SSN of a deceased individual in December 2008—at least a month after State claimed to have implemented the control that was designed to stop this type of passport fraud.

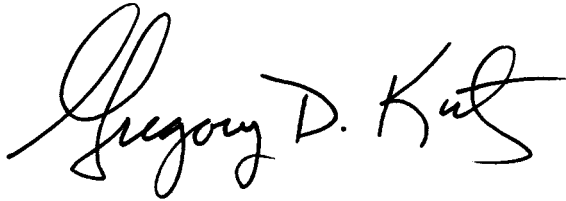
State officials also provided clarification of certain technical matters, which we have incorporated into this letter, as appropriate.

We are sending copies of this correspondence to the Secretary of State and other interested parties. This correspondence will also be available on the GAO Web site at <http://www.gao.gov>. If you or your staff have any questions concerning this correspondence, please contact Jess T. Ford at (202) 512-4268 or fordj@gao.gov, or Gregory Kutz at (202) 512-6722 or kutzg@gao.gov. Contact points for our Offices of

Congressional Relations and Public Affairs may be found on the last page of this correspondence.

A handwritten signature in black ink that reads "Jess T. Ford". The signature is written in a cursive style with a large, looping initial "J".

Jess T. Ford
Director
International Affairs and Trade

A handwritten signature in black ink that reads "Gregory D. Kutz". The signature is written in a cursive style with a large, looping initial "G".

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

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