GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 27, 2010

The Honorable Benjamin L. Cardin
Chairman
Subcommittee on Terrorism and Homeland Security
Committee on the Judiciary
United States Senate

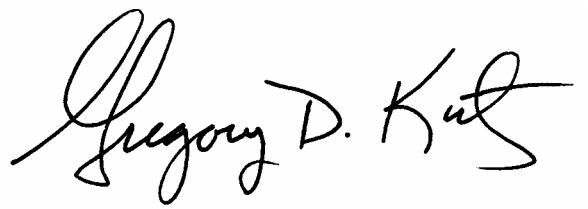
Subject: *Posthearing Responses to July 29, 2010, Hearing on the Passport Issuance Process: Closing the Door to Fraud, Part II*

Dear Mr. Chairman:

On July 29, 2010, we testified before your subcommittee at a hearing entitled *The Passport Issuance Process: Closing the Door to Fraud, Part II*. This letter responds to your request that GAO respond to a number of post-hearing questions. The questions and our answers are provided in the enclosure. The responses are based on work associated with previously issued GAO products, which were conducted in accordance with generally accepted government auditing standards and investigative standards from the Council of the Inspectors General on Integrity and Efficiency. We did not obtain comments from the Department of State.

If you have any further questions or would like to discuss these responses, please call me on (202) 512-6722.

Sincerely yours,



Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

Enclosure-1

Responses to Questions for the Record
Subcommittee on Terrorism and Homeland Security,
Committee on the Judiciary
The Passport Issuance Process: Closing the Door to Fraud, Part II
July 29, 2010

1. ***The Passport Identity Verification Act.***

   a. Does GAO support the Passport Identity Verification Act (PIVA), S.3666?

   b. Does the GAO agree that if PIVA is enacted, it will greatly improve the State Department's (State) ability to verify the identity of a passport applicant and detect passport fraud?

Answer:

a. We support the Passport Identity Verification Act.

b. We agree that if PIVA is properly implemented and consistently applied, it should enhance State's ability to verify the identity of passport applicants. According to State, limited access to relevant federal and state level agencies' records, because privacy concerns and the fact that State is not a law enforcement agency, has been a long-standing vulnerability in the passport issuance process. For example, State officials told us that limited access to such records enabled GAO to obtain the four genuine passports we reported in our March 2009 report. According to State, passport specialists did not wait for the results of a required Social Security Administration (SSA) database check before approving our fraudulent applications; further, in all four of our tests State failed to identify the fraudulent birth certificates we used. We have also reported that State has difficulty verifying driver's license information presented by passport applicants. Improving State's access to citizenship and identity information contained in databases maintained by relevant federal, state, local governments, private entities, or other organizations, to verify the authenticity of passport applicants' information, as called for in PIVA, should strengthen the State Department's ability detect fraud during the passport issuance process.

2. ***GAO's 2009 Recommendations.*** **In its May 2009 testimony, GAO made a number of recommendations with respect to changes the State Department needed to make to the passport issuance process. Please list those recommendations and the degree to which the State Department has implemented them.**

Answer:

In our May 2009 testimony, we suggested that the Secretary of State take the following corrective actions to address vulnerabilities in the passport issuance process:

1. **Improve the training and resources available to passport-acceptance-facility employees for detecting passport fraud, especially related to detecting counterfeit documents.**

   In Progress. State told us that it has established an Acceptance Facility Oversight Program (AFOP). The goal of the program is to develop an integrated database that will provide enhanced statistics to evaluate, track, and monitor acceptance facility performance. To do this, program analysts monitor, inspect, and report acceptance facility adherence to Passport Services' policies, practices, and procedures. In addition, the program includes enhanced Web-based and classroom training for non-State Department acceptance agents at the 9,400 designated facilities where the general public may apply for a U.S. passport. While the program presents some worthy goals, there is no indication that it will provide the Postal Service with the necessary training and resources to detect counterfeit documents, such as fraudulent drivers' licenses, submitted by passports applicants. Our most recent test shows that passport-acceptance-facility employees continue to have problems identifying counterfeit documents.

2. **For applications containing an SSN, establish a process whereby passport specialists are unable 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.**

   No Progress. Based on the results of our most recent tests of State's passport issuance process, State has not made progress on this recommendation. Similar to our first series of tests, five of the bogus applications that we submitted in our most recent tests were based on information and SSNs we had previously obtained from the SSA for the purpose of conducting undercover investigations. State immediately detected that two of the applications contained SSNs that did not match SSA data but failed to crosscheck the SSNs in the three remaining applications before they were approved for passport issuance. If State had taken sufficient action to implement this recommendation, it would have detected the erroneous SSNs in the remaining three passport applications before they were approved for passport issuance.

3. **Explore commercial options for performing real-time checks of the validity of SSNs and other information included in applications.**

   No Progress. Our most recent testing shows that State still does not conduct real time checks of the validity of SSNs and other information included in applications. If State had implemented this recommendation, it would have likely detected all seven of our passport applications as fraudulent as they all contained recently issued SSNs, counterfeit birth certificates, and counterfeit or fraudulently obtained drivers' licenses. Anecdotally, State showed some ability to conduct searches of SSNs and other identity information using commercial software such as LexisNexis, which it used to conduct research on our multiple addresses, SSNs, and other identifying information. However, this research was generally conducted only after State discovered our tests and realized that it had issued passports based on erroneous application information.

4. **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.**

   Implemented. According to State, this recommendation has been implemented and will remain a part of its ongoing efforts to strengthen the passport issuance process. In September 2009, State launched "red team" testing through the Passport Integrity Testing and Training Program (PITT). As of April 2010, three fraudulent passport applications were submitted by Diplomatic Security personnel with accompanying counterfeit birth certificates; of these, two applications were submitted through passport acceptance facilities and one was submitted at a passport agency public counter. State indicated that in each case, the fraudulent passport applications were detected by Passport Services.

5. **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.**

   In Progress. State has increased data and information-sharing with relevant federal, state, local, and private organizations that possess information. According to State, it has deployed the National Law Enforcement Telecommunications System Information Sharing Network, Inc. (NLETS) system, which gives the State Department access to drivers' license data for 49 States (South Dakota has declined to participate), Puerto Rico, and the District of Columbia. To verify questionable birth certificates, State's Fraud Prevention Managers employ the Electronic Verification of Vital Events (EVVE) system available through the National Association for Public Health Statistics and Information Systems (NAPHSIS). We do not know the effectiveness of these systems. Nor do we know the extent to which they are utilized by State during the passport issuance process. Our recent tests show that State does not consistently conduct data verification at the front-end of the passport application process because all of the applications for which passports were issued contained counterfeit or fraudulently obtained birth certificates and drivers' licenses.