GAO

United States Government Accountability Office

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
Thursday, July 29, 2010

STATE DEPARTMENT

Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud

Statement of Gregory Kutz, Managing Director
Forensic Audits and Special Investigations

GAO
Accountability * Integrity * Reliability

GAO-10-922T

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

July 29, 2010

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-10-922T, a testimony before the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

STATE DEPARTMENT

Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud

Why GAO Did This Study

A U.S. passport is one of the most sought after travel documents in the world, allowing its holder entrance into the United States and many other countries. People attempting to obtain a U.S. passport illegally often seek to use the guise of a U.S. citizen to conceal their involvement with more serious crimes, such as terrorism, drug trafficking, money laundering, or murder.

In March 2009, GAO reported on weaknesses in State's passport issuance process that could allow a terrorist or criminal to fraudulently acquire a genuine U.S. passport. Specifically, GAO easily obtained four genuine passports from State using counterfeit documents. In April 2009, GAO suggested that State take 5 corrective actions based on these undercover tests and State acknowledged those corrective actions. GAO was asked to perform additional proactive testing of State's passport issuance process to determine if it continues to be vulnerable to fraud.

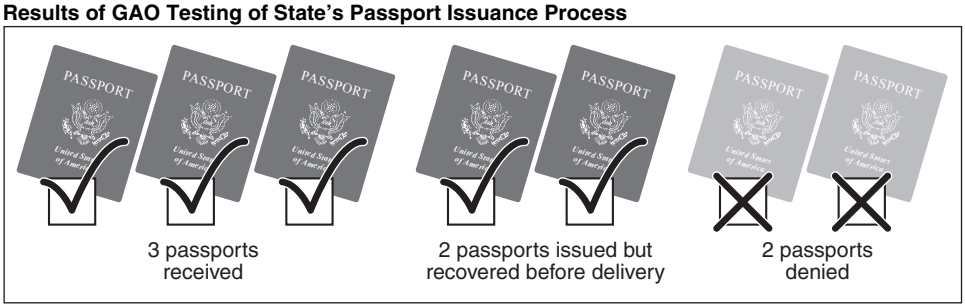
To do this work, GAO applied for seven U.S. passports using counterfeit or fraudulently obtained documents, such as driver's licenses and birth certificates, to simulate scenarios based on identity theft. GAO created documents for seven fictitious or deceased individuals using off-the-shelf, commercially available hardware, software, and materials. Undercover investigators applied for passports at six U.S. Postal Service locations and one State-run passport office.

View GAO-10-922T or key components.
For more information, contact Gregory Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

State's passport issuance process continues to be vulnerable to fraud, as the agency issued five of the seven passports GAO attempted to fraudulently obtain. While there were multiple indicators of fraud and identity theft in each application, State identified only two as fraudulent during its adjudication process and mailed five genuine U.S. passports to undercover GAO mailboxes. GAO successfully obtained three of these passports, but State had the remaining two recovered from the mail before they were delivered. According to State officials, the agency discovered—after its adjudication process—that the two passports were part of GAO testing when they were linked to one of the passport applications it initially denied. State officials told GAO that they used facial recognition technology—which they could have also used during the adjudication process—to identify the two remaining applications.

Results of GAO Testing of State's Passport Issuance Process



Source: GAO.

GAO's tests show that State does not consistently use data verification and counterfeit detection techniques in its passport issuance process. Of the five passports it issued, State did not recognize discrepancies and suspicious indicators within each application. Some examples include: passport photos of the same investigator on multiple applications; a 62 year-old applicant using a Social Security number issued in 2009; passport and driver's license photos showing about a 10 year age difference; and the use of a California mailing address, a West Virginia permanent address and driver's license address, and a Washington, D.C. phone number in the same application. These were fraud indicators that should have been identified and questioned by State. State also failed to crosscheck the bogus citizenship and identity documents in the applications against the same databases that it later used to detect GAO's other fraudulent applications. State used facial recognition technology to identify the photos of GAO undercover investigators and to stop the subsequent delivery of two passports but not to detect fraud in the three applications that GAO received, which all contained a passport photo of the same investigator.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss the results of our investigation of the State Department's (State) passport issuance process. My testimony today highlights the results of our most recent tests of this process, which we have previously shown to be vulnerable to fraud.[1] According to State, over 13 million U.S. passports were issued in fiscal year 2009. U.S. passports are one of the most sought after travel documents in the world, allowing its holders entrance into the United States and visa-free passage into many other countries. People attempting to obtain a U.S. passport illegally are often seeking to use the guise of a U.S. citizen to conceal their involvement with more serious crimes, such as terrorism, narcotics trafficking, money laundering, and murder. For example, in December 2009, an alleged leader of a white supremacist gang was sentenced to 3 years in federal prison for making a false statement on a passport application in order to flee a double-murder investigation.

In March 2009, we reported on weaknesses in State's passport issuance process that could allow a terrorist or criminal to fraudulently acquire a genuine U.S. passport. Specifically, we easily obtained four genuine passports from State using counterfeit and fraudulently obtained documents. Over the years State has taken steps to protect against the fraudulent use of U.S. passports by, for example, issuing only electronic passports.[2] However, terrorists and other criminals could still circumvent these security measures by using stolen identities and fraudulent breeder documents,[3] such as birth certificates and drivers' licenses, to obtain genuine passports. For example, in late 2006, State's Bureau of Diplomatic Security initiated a multiyear investigation, uncovering a criminal

[1] GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C.: Mar. 13, 2009). GAO, *Addressing Significant Vulnerabilities in the Department of State's Passport Issuance Process*, GAO-09-583R, (Washington, D.C.: April, 13, 2009). GAO, *State Department: Significant Vulnerabilities in the Passport Issuance Process*, GAO-09-681T (Washington, D.C.: May 5, 2009).

[2] The electronic passport, or e-passport, is like the traditional passport booklet with the addition of a radio frequency identification (RFID) chip embedded in the back cover, which provides for electronic storage of biographical and biometric data. This addition allows for a comparison of the photo in the passport with the photo in the chip, and can provide greater assurance that the photo, as well as the biographic data, has not been altered or counterfeited.

[3] A breeder document is an ID document issued to support a person's identity and obtain another document of privilege or of greater perceived value.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

enterprise through which Jamaican and West African nationals bought counterfeit New York City birth certificates to fraudulently obtain U.S. passports. As a result, agents confiscated 17 fraudulently obtained U.S. passports and intercepted 10 fraudulent passport applications. Further, the fraudulent use of Puerto Rican birth certificates to obtain U.S. passports was so widespread that in December 2009, the Puerto Rican government enacted a law that invalidates all birth certificates issued before July 1, 2010.[4]

This testimony responds to your request that we perform additional proactive testing of State's passport issuance process to determine whether it continues to be vulnerable to fraud. To perform this work, we designed three test scenarios—similar to those we used in our previous testing—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.[5] We then applied for seven genuine U.S. passports and supported our applications with counterfeit or fraudulently obtained documents, such as birth certificates and drivers' licenses, and the Social Security numbers (SSN) and identities of fictitious or deceased individuals. We fabricated these documents using publicly available software, hardware, and materials.

Our seven tests simulate an individual stealing another person's identity and using it to obtain a passport. Five of our tests were based on information and SSNs we had previously obtained from the Social Security Administration (SSA) for the purpose of conducting undercover tests. One of these included the identity and SSN of a five year old child to simulate a malicious individual stealing the identity of a real child to get a passport. Finally, in two other tests, we used the identities of individuals who died in 1966 and 1969. For six tests, we submitted our passport applications and supporting materials at United States Postal Services (USPS) locations that accept passport applications. For the other test, we submitted our application and materials at State's regional Washington, D.C., passport-

[4] The law was based on collaboration with State and the Department of Homeland Security (DHS) to address the fraudulent use of Puerto Rico–issued birth certificates to unlawfully obtain U.S. passports, Social Security benefits, and other federal services. A June 2010 amendment to the law extends the validity of these birth certificates through September 30, 2010, to provide a transition for those applying for new documents.

[5] Identity theft occurs when an individual steals another individual's personal identifying information and uses it fraudulently.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

issuing office. We also briefed State officials on the results of our investigation and discussed their actions on our tests.

We conducted our work from January 2010 through July 2010 in accordance with quality standards for investigations as set forth by the Council of Inspectors General on Integrity and Efficiency.

Background

A U.S. passport is not only a travel document but also an official verification of the bearer's origin, identity, and nationality. Each day, Americans submit them as identification to board international flights, obtain drivers' licenses, cross the border from the United States into Canada and Mexico, apply for loans, and verify their employability. To acquire a U.S. passport for the first time, an applicant must provide evidence of citizenship, or non-citizen nationality,[6] such as a certificate of birth in the United States or a naturalization certificate, and a valid government-issued identification document that includes a photograph or physical description of the holder (most commonly a state-issued driver's license or identity card).[7]

Most passport applications are submitted by mail or in-person at one of almost 9,400 passport application acceptance facilities nationwide. The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document matches the applicant. Then, through adjudication, passport examiners determine whether State 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 or non-citizen nationality.

Since 2005, we have issued several reports on fraud vulnerabilities within the passport issuance process and the subsequent actions taken by State

[6] Non-citizen nationals, such as individuals born in American Samoa, comprise only a small portion of eligible passport recipients.

[7] Valid government-issued documents include, for example, state drivers' licenses, state identification cards, or military identification.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

to prevent individuals from fraudulently securing passports.[8] For example, we reported that identity theft was among the most common means used to commit passport fraud. In March 2009, we reported that our covert testing of State's passport issuance process demonstrated how malicious individuals might use identity theft to obtain genuine U.S. passports. Through our work, we have identified two major areas of vulnerability in State's passport issuance process.

- Passport acceptance agents and passport examiners have accepted counterfeit or fraudulently acquired genuine documents as proof of identification and citizenship. We reported in March 2009 that State issued four genuine U.S. passports to GAO investigators, even though the applications that we submitted contained bogus information and were supported by counterfeit drivers' licenses and birth certificates.[9] The sheer variety of documents that are eligible to prove citizenship and identity also complicate State's verification efforts.

- State's limited access to information from other federal and state agencies hampers its ability to ensure that supporting documents belong to the bearer. In 2005 we reported that the information State used from SSA to corroborate SSNs was limited and outdated.[10] Although State and SSA had signed a memorandum in April 2004 giving State access to SSA's main database, the memorandum had not been implemented. Moreover, the memorandum did not include access to SSA's death records, though State officials said they were exploring the possibility of obtaining these records. Yet, in one case from our covert testing in 2009, we obtained a U.S. passport using the SSN of a man who died in 1965. In response to our prior findings, State officials said that the lack of an automated check against SSA death records was a long-standing vulnerability, but noted that Passport Services had recently purchased a subscription to the Death Master File, which included weekly updates of deaths recorded by SSA. State also indicated that federal agencies limit its access to records due to

---

[8] GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-477 (Washington, D.C.: May 20, 2005); GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-853T, (Washington, D.C.: June 29, 2005); 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); and GAO-09-447.

[9] GAO-09-447.

[10] GAO-05-477.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

privacy concerns and the fact that State is not a law enforcement agency. For example, it could not conduct real-time authentication of the birth certificates presented by passport applicants. The agency added that these documents present an exceptional challenge to fraud detection efforts, due to the thousands of different acceptable formats that the documents can be presented in. It further indicated that there are also difficulties with verifying the authenticity of drivers' licenses.

Covert Testing of State's Passport Issuance Process Shows That Vulnerabilities Remain

State's passport issuance process continues to be vulnerable to fraud, as the agency issued five of the seven passports GAO attempted to fraudulently obtain. Despite multiple indicators of fraud and identity theft in each application, State identified only two as fraudulent during its adjudication process and mailed five genuine U.S. passports to undercover GAO mailboxes. GAO successfully obtained three of these passports, but State had two others recovered from the mail before they were delivered. According to State officials, the agency discovered—after its adjudication process—that the two passports were part of GAO testing when they were linked to one of the passport applications it initially denied. State officials told us that they used facial recognition technology [11]—which it could have also used during the adjudication process—to identify our two remaining applications.

According to State, one of our applications was denied in April 2010 during processing at the National Processing Center in New Hampshire by an examiner who was suspicious that the application in totality was likely an "imposter." The examiner sent the file to a fraud manager in Florida who subsequently determined that the Florida birth certificate was counterfeit. State detected the second fraudulent application after the SSN used was flagged as recently issued by SSA. This application was then sent to the same fraud manager in Florida who processed the first application, since they both contained Florida birth certificates. State officials indicated that they then uncovered GAO's undercover tests by crosschecking the fraudulent Florida birth certificate with the state's Bureau of Vital Statistics.

[11] Facial recognition technology is used to compare an individual's face or photo against multiple "galleries" of images. According to State, staff trained in facial comparison techniques use this technology to help prevent the issuance of U.S. passports to individuals using false identities and individuals who should be denied passports for other legal reasons.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

After State discovered our undercover test, the agency used methods and resources not typically utilized to detect fraud during the normal passport adjudication process to identify our remaining tests. For example, according to State officials, they subsequently identified the two remaining GAO applications by using facial recognition technology to search for the photos of the applicants, who were our undercover investigators. State could have used the very same technology to detect fraud in the three applications for passports that we received, because all three passports contained the photo of the same GAO investigator. One of the passports that were recovered after issuance also included the photo of the same investigator.

Our most recent tests show that State does not consistently use data verification and counterfeit detection techniques in its passport issuance process. Of the five passports issued, State failed to crosscheck the bogus citizenship and identity documents in the applications against the same databases that it later used to detect our other fraudulent applications. In addition, despite using facial recognition technology to identify the photos of our undercover investigators and to stop the subsequent delivery of two passports, State did not use the technology to detect fraud in the three applications for passports that we received, which all contained a passport photo of the same investigator. Table 1 and the text that follows provide more detail about each of our tests.

Table 1: Results of GAO Undercover Testing of State's Passport Issuance Process

Test number	Date of Application	State Where Application Filed	Fraud Indicators	Date of Disposition	Final Disposition
1	3/10/10	Washington	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	3/24/10	Passport Issued
2	3/31/10	California	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	5/31/10	Detected, No Passport Issued

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

Test number	Date of Application	State Where Application Filed	Fraud Indicators	Date of Disposition	Final Disposition
3	4/19/10	Washington, D.C.	• Identity of a 65 year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit D.C. driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	4/20/10	Passport Issued
4	4/22/10	California	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	5/10/10	Passport Issued
5	5/4/10	Illinois	• SSN of a child being used by a 55-year-old applicant • Counterfeit FL birth certificate • Counterfeit WV driver's license • Different height on application and license • Same photo used in multiple passports	Unknown	Detected, No Passport Issued—Linked to GAO Covert Testing
6	5/25/10	Georgia	• Identity of a deceased individual • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	6/15/10	Recovered After Issuance and Determination That GAO was Conducting a Covert Test
7	5/26/10	New York	• Identity of a deceased individual • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	6/11/10	Recovered After Issuance and Determination That GAO was Conducting a Covert Test

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

Test One (Washington): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual

State issued a genuine passport even though the application contained multiple indicators that should have raised suspicion of fraud, either independently or in aggregate. First, this application included both a counterfeit Florida birth certificate and West Virginia driver's license, both using the same fictitious name that was on the application. If State had confirmed the legitimacy of these documents, it would have easily discovered that they were bogus and thus, not representative of the true identity of the bearer. Second, we utilized an SSN that was recently issued to us by the SSA. If State had authenticated the SSN, it would have detected the fact that its issue date did not closely coincide with the date of birth and age of the U.S. citizen represented in the application. Specifically, the applicant listed was a 62-year-old man born in 1948 while the SSN was issued by SSA in 2009. Finally, State did not question discrepancies between our addresses which included a permanent home address located in West Virginia and a mailing address in Seattle, Washington. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

Test Two (California): State Detected Our Fraudulent Application Before Issuance

State denied this passport after identifying certain discrepancies and indicators of identity theft and fraud that we included in the application. According to State, this fraudulent application was first detected when the applicant's identity information did not match SSA's records. The application was then submitted to an examiner, who determined that our Florida birth certificate was fraudulent after checking it against Florida Bureau of Vital Statistics records. State also identified physical properties of the document that were inconsistent with an original. In addition, State checked our bogus West Virginia driver's license against the National Law Enforcement Telecommunications System (NLETS), which showed that the license did not belong to the bearer.

Test Three (District of Columbia): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual

State issued a genuine passport even though the application contained multiple indicators and discrepancies that should have raised red flags for identity theft and fraud. Our investigator went to the U.S. Department of State Passport Office in Washington, D.C., which provides expedited passport services to applicants scheduled to travel out of the country within 14 days from the date of application. The State employee made a line-by-line examination of the application to make sure that the information coincided with what was provided to him, on the bogus Florida birth certificate and District of Columbia driver's license. Both documents contained the same fictitious name that was used on the application. However, if State had crosschecked the information from

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

these two bogus documents against the same records that it did in the previous case, it could have discovered that neither were representative of the bearer. Further, if State officials had checked the SSN in the application, State would have concluded that it was recently issued and did not coincide with the date of birth represented in the application. In addition, our application indicated that our applicant's height was 5' 10" while his bogus driver's license showed a height of 6'. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport. The following day, our investigator returned to the same location and was issued a genuine U.S. passport.

Test Four (California): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual

State again issued a genuine passport even though the application contained multiple indicators and discrepancies that should have raised red flags for identity theft and fraud. This application also included a counterfeit Florida birth certificate and West Virginia driver's license, both in the same fictitious name that was used on the application. If State had adequately corroborated the information from these two bogus documents against the same records that it did in case number two, it could have discovered that the documents were counterfeit and not representative of the bearer. In addition, if State had adequately verified the SSN in the application, it would have found that the recent issue date did not coincide with the age or date of birth represented in the application. State also did not identify about a 10 year age difference between the applicant's passport photo and the photo in his driver's license. Finally, the application included suspicious addresses and contact information—a California mailing address, a permanent and driver's license address from West Virginia and telephone number from the District of Columbia. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

Test Five (Illinois): State Detected Our Fraudulent Application Before Issuance

State identified the fraud indicators and discrepancies that we included in this test and did not issue a passport. In addition, the agency identified this application as a GAO undercover test. First, State identified a major discrepancy with the SSN in our application. When our investigator spoke with a State employee about the status of his application, he was told that the birth year in his application did not match SSA records. In our investigator's fabricated explanation, he explained that he was recently a victim of identity theft and had a new SSN issued. Second, the agency determined that our Florida birth certificate was fraudulent after its check against Florida Bureau of Vital Statistics records indicated that the document was counterfeit. State also identified physical properties of the

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

document that were inconsistent with an original. Finally, State questioned why the application was filed in Illinois yet listed a mailing, permanent, and driver's license address from West Virginia.

Test Six (Georgia): State Issued Passport Using the Identity of a Deceased Individual But Prevented Its Delivery

State issued a passport for this application even though it contained multiple indicators of fraud. However, after discovering our testing through our fifth application, it subjected this application to further review and recovered the passport from the USPS before it was delivered. Before the application was discovered as a part of a GAO test, State never identified any of the fraud indicators that we included in the application. Officials stated that facial recognition technology allowed them to discover that the photograph in this application was the same used in previous applications. State then checked our bogus West Virginia driver's license against NLETS, which showed that the license belonged to a person other than the bearer. State officials never questioned why the application was filed in Georgia yet listed a mailing, permanent, and driver's license address from West Virginia and phone number from the District of Columbia. State also failed to identify the misspelling of the city in our West Virginia license and discrepancies with the zip code information on our passport application. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

Test Seven (New York): State Issued Passport Using the Identity of a Deceased Individual But Prevented Its Delivery

As with our sixth test, State issued a passport for this application but prevented its delivery after using facial recognition technology to link the photo to one used in previous applications—again, after discovering our undercover testing. Only after discovering our testing did State check our bogus West Virginia driver's license against NLETS, which showed that the license belonged to a person other than the bearer. If State had checked this license prior to issuing a passport, it would have discovered discrepancies regarding information on the license including the misspelling of the city. Further, State never questioned why the application was filed in New York yet listed a Maryland mailing address and a permanent and driver's license address from West Virginia, prior to issuing the passport that it later revoked. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

In conclusion, Mr. Chairman, the integrity of the U.S. passport is an essential component of State's efforts to help protect U.S. citizens from those who would harm the United States. Over the past several years, we

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

have reported that State has failed to effectively address the vulnerabilities in the passport issuance process. Our recent tests show that there was improvement in State's adjudication process because State was able to identify 2 of our 7 passport applications as fraudulent and halted the issuance of those passports. However, our testing also confirmed that State continues to have significant vulnerabilities and systemic issues in its passport issuance process. We look forward to continuing to work with this Subcommittee and State to improve passport fraud prevention controls.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you may have at this time.

Contacts and Acknowledgements

For further information regarding this testimony, please contact Greg Kutz at (202) 512-6722 or kutzg@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Andy O'Connell, Assistant Director; John Cooney, Assistant Director; Matthew Valenta, Assistant Director; Lerone Reid, Analyst-In-Charge; Jason Kelly; Robert Heilman; James Murphy; and Timothy Walker.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

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.

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)

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

AILA InfoNet Doc. No. 10073064. (Posted 07/30/10)
Please Print on Recycled Paper