United States General Accounting Office

GAO

Testimony

Before the Senate Committee on Finance

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, September 9, 2003

SECURITY

Counterfeit Identification and Identification Fraud Raise Security Concerns

Statement of Robert J. Cramer, Managing Director
Office of Special Investigations

GAO-03-1147T

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today to summarize some of our recent investigations that demonstrate security vulnerabilities that exist because counterfeit identification can be easily produced and used to create fraudulent identities.

My testimony today is based in part on the recently issued restricted report *Security*: *Vulnerabilities Found in Driver's License Applications Process*.[1] My remarks also encompass results from security tests we have performed over the past 3 years. These tests revealed security weaknesses at federal buildings and other facilities, airports and our nation's borders, and exposed identity fraud vulnerabilities in both the Social Security number (SSN) application process and in the administration of federal gun control laws. (See app. I for a synopsis of the tests we have conducted since 2000.) A number of these problems have been addressed by the responsible agencies.

In conducting these tests, we created fictitious identities and counterfeit identification documents, such as driver's licenses, birth certificates, and Social Security cards. We did this using inexpensive software and hardware that are readily available to any purchaser.

In summary, we found that (1) government officials generally did not recognize the documents we presented as counterfeits, (2) some government officials failed to follow security procedures and were not alert to the possibility of identity fraud, and (3) identity verification procedures are inadequate. Our investigations revealed that homeland security is vulnerable to identity fraud and, unless action is taken, individuals who intend to cause harm can easily exploit these vulnerabilities. Additionally, identify fraud has a range of other consequences including potential fraud in voting, obtaining credit and federal benefits, and in many other areas.

[1] U.S. General Accounting Office, *Security*: *Vulnerabilities Found in Driver's License Applications Process*, GAO-03-989RNI (Washington, D.C.: Sept. 9, 2003).

Government Officials Did Not Recognize Our Counterfeit Documents

During each of our tests, we found that government officials did not recognize that the documents we presented were counterfeit. For example, during our driver's license investigation, we used counterfeit driver's licenses to obtain genuine driver's licenses in seven states and the District of Columbia. Because motor vehicle department employees did not recognize as counterfeit the documents we presented, including out-of-state driver's licenses, they issued genuine licenses to our investigators. During our border security investigation, in which we used counterfeit driver's licenses and birth certificates to enter the United States, border inspectors never questioned the authenticity of the documents and our investigators encountered no difficulty entering the country. In another test, we obtained SSNs for fictitious children when investigators posed as parents of newborns and submitted counterfeit birth certificates and baptismal certificates. Additionally, we breached the security of airports and federal office buildings because no one questioned the authenticity of our counterfeit identification. Additional training of government personnel in the detection of counterfeit identification documents is sorely needed.

Some Government Officials Failed to Follow Security Procedures and Were Not Alert to the Possibility of Identity Fraud

We also discovered that some officials failed to follow security procedures and were not alert to the possibility of identity fraud. For example, we found that some security personnel did not look at photo identification. As a result, officials allowed one of our agents, who presented identification containing another person's photograph, to enter a federal building in Atlanta. Another investigator entered a federal building and obtained a building pass and an after hours access code from security personnel who did not follow procedures to verify his identity. In addition, this investigator was able to obtain a second feature added to the building pass that identified him as a law enforcement officer and permitted him to carry a firearm. Yet another investigator presented a counterfeit building pass to a security officer and obtained from the officer an access code used to enter the building after working hours.

Additionally, even motor vehicle department employees who recognized irregularities in the documents we submitted were not alert to the possibility of identity fraud. For example, one employee noticed that the birth date on an investigator's counterfeit birth certificate and other records did not match the birth date assigned to his SSN. Another employee questioned the validity of an investigator's birth certificate because of the texture of the paper and because it did not contain a seal. In each instance, however, employees who saw such irregularities returned

the documents to the investigators. In at least one of the states we visited, Department of Motor Vehicle (DMV) employees are required to confiscate documents that they suspect to be fraudulent and send a teletype alerting all state driver's license offices of the facts surrounding the questionable documentation. However, this policy was not followed.

Improved Verification Procedures Are Needed

Current verification procedures followed by border inspectors and firearms dealers often consist of what we call a "negative" check; that is, a database is queried for information about the specific name or other personal identifiers submitted. This process reveals whether the database contains information about the name submitted but does not verify the identity of the license applicant or the authenticity of the license presented. For example, we purchased firearms from licensed firearms dealers using counterfeit driver's licenses. The majority of firearms dealers we contacted complied with the then-existing federal and state law governing such purchases, including instant background checks required by the Brady Handgun Violence Prevention Act of 1993.[2] However, the instant background check only discloses whether the prospective purchaser is a person whose possession of a firearm would be unlawful. Consequently, if the prospective purchaser is using a fictitious identity, as our investigators did, an instant background check is not effective.

Our border security tests, in which we used counterfeit driver's licenses to enter the United States from various Western Hemisphere countries, point to the same problem. Because immigration regulations do not require U.S. citizens traveling from countries in the Western Hemisphere to show passports when entering the United States, persons entering the United States from such countries commonly present driver's licenses to border inspectors for identification purposes. However, border inspectors currently have no way of checking with the states to verify identity or to determine whether a driver's license is authentic.

Conclusion

A driver's license is the most commonly accepted document used to identify an individual. The weaknesses we found during these investigations clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify identity

[2] 18 U.S.C. § 922(t).

and to determine whether out-of-state driver's licenses presented to them are authentic. Improved verification procedures could minimize vulnerabilities presented when government officials do not recognize counterfeit documents or are not alert to the possibility of identity fraud. Also, government officials who review identification documents need training and need to be more vigilant for identification fraud.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other members of the committee may have at this time.

Contacts and Acknowledgement

For further information regarding this testimony, please contact Robert Cramer, Managing Director, or Ronald Malfi, Director, Office of Special Investigations at (202) 512-6722. Individuals making key contributions to this testimony include Dan Bertoni, John Cooney, Jennifer Costello, Barbara Lewis, and George Ogilvie.

Summary of Recent Reports and Testimony

Security: Vulnerabilities Found in Driver's License Applications Process

From July 2002 through May 2003, Office of Special Investigations (OSI) investigators visited state driver's licensing agencies (hereinafter referred to as DMVs) in Virginia, Maryland, the District of Columbia, South Carolina, Arizona, California, Michigan, and New York. Because the focus of this test was to determine whether DMVs would issue driver's licenses based on counterfeit documents, we obtained valid undercover Social Security Numbers (SSN) from the Social Security Administration (SSA) that would be verified by SSA if queried by DMV employees.[1] We were successful in obtaining authentic but fraudulent driver's licenses using fictitious names supported by counterfeit documents, including counterfeit out-of-state driver's licenses. We used the same fictitious names, birth dates, and SSN's at most of the locations without detection, and we used the same counterfeit driver's licenses in all states except Maryland and Virginia.

During the course of this investigation, we found that DMV employees generally did not recognize our counterfeit driver's licenses. Other DMV employees recognized irregularities in the documents we submitted but they routinely returned the documents to us. This investigation revealed that the current system in the 26 states that rely solely on visual inspection of documents to detect counterfeits is vulnerable and can easily be exploited.[2]

[1] SSA provides a verification service that allows state DMVs to verify the name, SSN, and date of birth of an applicant. While 26 states, including one state we visited, rely primarily on visual inspection of documents submitted by driver's license applicants to detect counterfeits, 24 states and the District of Columbia now use SSA's verification service. Nevertheless, criminals can steal the identities of individuals and obtain driver's licenses using counterfeit documents containing those individual SSNs. In addition, our investigative work has demonstrated that criminals can create documentation for fictitious individuals and apply for and receive valid SSNs, which can be used on counterfeit documents to obtain a driver's licenses.

[2] GAO-03-989RNI.

Social Security Numbers: Ensuring the Integrity of the SSN

In May 2003, we were able to prove the ease with which individuals can obtain SSNs by exploiting SSA's current processes. Working in an undercover capacity, we used counterfeit identification documents to obtain valid SSNs from SSA for two fictitious infants. By posing as parents of newborns, we obtained the first SSN by applying in person at a SSA field office using a counterfeit birth certificate and baptismal certificate. Using similar documents, we obtained a second SSN by submitting the counterfeit documents through the mail. In both cases, SSA staff accepted our counterfeit documents as valid. Thus, SSA's current policies relating to issuing SSNs to children under the age of one expose the agency to fraud.[3] SSA officials stated that they are reevaluating their policy.

During a hearing on July 10, 2003, we discussed our visits to DMVs in two states where we obtained authentic but fraudulent driver's licenses using the names, SSNs, and dates of birth of individuals listed on SSA's Master Death file. The Master Death file is publicly available and contains SSN's of deceased individuals. The two states we visited are among several states that rely on visual verification of identification documents and use SSA's batch process verification service, which allows DMVs to verify the name, SSN, and date of birth of an applicant but does not check the applicant's information against SSA's Master Death file.[4] Further, our analysis of 1 month of transactions submitted to SSA by one of these states showed that driver's licenses and identification cards had been issued to 41 individuals who used the names, SSNs, and dates of birth of persons listed as deceased in SSA's records. Our ability to obtain driver's licenses in the two states we visited and the 41 cases identified in our analysis demonstrate a significant gap in SSA's verification service to the states.

[3] U.S. General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN*, GAO-03-941T (Washington, D.C.: July 10, 2003).

[4] SSA also offers an on-line process to states that includes matching the applicants' information against the Master Death file.

Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected

From September 2002 through May 2003, we used counterfeit documentation, including counterfeit driver's licenses and fictitious names, to enter the United States from Jamaica, Barbados, Mexico, and Canada. Bureau of Immigration and Customs Enforcement (BICE) staff never questioned the authenticity of the counterfeit documents, and our investigators encountered no difficulty entering the country using them. Although BICE inspects millions of people who enter the United States and detects thousands of individuals who attempt to enter illegally each year, the results of our work indicate that BICE inspectors are not readily able to detect counterfeit identification documents.[5]

Security Breaches at Federal Buildings in Atlanta, Georgia

In February and March of 2002, we breached the security of four federal office buildings in the Atlanta area using counterfeit law enforcement credentials to obtain genuine building passes, which we then counterfeited. In addition, we were able to obtain building passes that indicated that we were authorized to carry firearms in the buildings. As a result, several investigators, including one carrying a briefcase or package, bypassed the magnetometers and X-ray machines and used the counterfeit building passes to enter several buildings. They were able to move freely and extensively throughout these facilities during day and evening hours and were not challenged by anyone. In addition, they obtained a security guard's after-hours access code when they presented the counterfeit building passes.

[5] U.S. General Accounting Office, *Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected*, GAO-03-713T (Washington, D.C.: May 13, 2003).

During this investigation we found that these buildings had security systems in place to screen visitors and valises. These systems included the use of magnetometers and X-ray machines at security checkpoints. The security systems also required that employees wear building passes for identification, which allowed them to bypass the magnetometers and X-ray machines. However, we were able to gain access because the employee responsible for issuing building passes did not follow existing procedures to verify the investigator's identity. Further, other security personnel failed to identify the counterfeit building passes. The Federal Protective Service, which is responsible for security at federal buildings, took action as a result of the weaknesses we identified.[6]

Firearms Purchased from Federal Firearms Licensees Using Bogus Identification

From October 2000 through February 2001, we used counterfeit driver's licenses with fictitious identifiers to purchase firearms from federal firearm licensees in five states—Virginia, West Virginia, Montana, New Mexico, and Arizona. The weapons purchased included (1) a 9mm stainless semiautomatic pistol, (2) a .380 semiautomatic pistol, (3) a 7.62mm Russian-manufactured rifle, (4) a .22 caliber semiautomatic rifle, (5) a 9mm semiautomatic pistol, and (6) a .25 caliber semiautomatic pistol.

The five states in which we purchased firearms conformed to the Brady Handgun Violence Prevention Act of 1993[7] by requiring instant background checks. For the most part, the federal firearm licensees we contacted adhered to then-existing federal and state laws regarding such purchases, including the instant background checks. Because we used counterfeit driver's licenses and fictitious identities there was no negative information in the system about the names we created.[8]

[6] U.S. General Accounting Office, *Security Breaches at Federal Buildings in Atlanta, Georgia*, GAO-02-668T (Washington, D.C.: Apr. 30, 2002).

[7] 18 U.S.C. § 922(t).

[8] U.S. General Accounting Office, *Firearms: Purchased from Federal Firearm Licensees Using Bogus Identification*, GAO-01-427 (Washington, D.C.: Mar. 19, 2001).

Purchase of Firearms Using a Counterfeit Federal Firearms License

In January 2002, we purchased a firearm from a licensed federal firearms dealer using a counterfeit federal firearms license. We established a fictitious sporting goods company in Virginia by using a legitimate federal firearms license and altering it to insert the name and address of our fictitious business. We then contacted a legitimate federal firearms dealer in Texas, posing as an individual wanting to purchase a .32 caliber semiautomatic pistol and have it shipped to Virginia. When the dealer stated that he could only mail the pistol to another federal firearms licensee, another investigator called the dealer, represented himself to be a licensed federal firearms dealer, and faxed a copy of a counterfeit license. The Texas dealer accepted the license and mailed the pistol. We also reported on two instances in which individuals purchased firearms using counterfeit or altered federal firearms licenses.[9]

Security: Breaches at Federal Agencies and Airports

In April and May of 2000, OSI investigators breached security at 19 federal sites and 2 commercial airports. Our investigators carried bogus badges and credentials, declared themselves to be armed law enforcement officers, and gained entry while avoiding screening procedures, including magnetometers and X-ray machines. At least one investigator carried a valise. Sixteen of the sites contained the offices of cabinet secretaries or agency heads. At 15 of these sites, investigators were able to stand immediately outside the suites of the cabinet secretary or agency head. In five instances, we were able to enter the cabinet secretary or agency head's suite. At the two airports we visited, investigators used tickets issued in fictitious names, declared themselves to be armed law enforcement officers, displayed their spurious badges and identification, and were issued "law enforcement" boarding passes by airline representatives. They then went to the security checkpoint and were waived around the magnetometers. Their valises were not screened. These investigations took place before September 11, 2001. Subsequently, federal agencies changed their policies to address the weaknesses we demonstrated.[10]

[9] U.S. General Accounting Office, *Purchase of Firearms Using a Counterfeit Federal Firearms* License, GAO-02-383R (Washington, D.C.: Mar. 13, 2002).

[10] U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (Washington, D.C.: May 25, 2000).

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548