

License to Hide:

Security Implications of America's Lax Driver's Licensing

Laws*

* This report has a special history. In 2002 and 2003 I participated in the Task Force on National Security in the Information Age convened by the Markle Foundation. It issued two important and highly valuable reports: *Protecting America's Freedom in the Information Age* (New York: Markle Foundation, 2002) and *Creating a Trusted Information Network for Homeland Security* (New York: Markle Foundation, 2003), both of which are available online at <http://www.markletaskforce.org>. I suggested to the Co-Chairs of the Task Force, Zoë Baird and James L. Barksdale, that they authorize the creation of a sub-group to study the issues discussed in this report. The sub-group on Reliable Identification for Homeland Protection and Collateral Gains was formed and I served as its chair. Its members included, Robert D. Atkinson, Stewart A. Baker, Eric Benhamou, William P. Crowell, David Farber, Mary McKinley, Paul Rosenzweig, Jeffrey Smith, James B. Steinberg, Paul Schott Stevens, and Michael Vatis. Following consultations with the members of the task force—especially William P. Crowell, Michael Vatis, and Robert D. Atkinson—I drafted a report that the members of the task force approved and which was included in the 2003 Markle publication. It naturally varied considerably from what I would have written on my own. Hence, although this report draws extensively on the work of the sub-group, it differs from it substantially and, above all, includes new primary data that I collected from the fifty states and the District of Columbia. I am indebted to Deirdre Mead for her excellent research assistance and to Jared Bloom for helping to prepare this report.

–Amitai Etzioni, The George Washington University

For more information, contact the Institute for Communitarian Policy Studies at comnet@gwu.edu or at (202)-994-8190.

I. Introduction

Fraudulent and falsified state driver's licenses remain easy to obtain and produce, despite the fact that these licenses are by far the most commonly used means for identifying people in the United States. As a result, major security programs such as the No Fly List, Terrorist Watch Lists, and, of course, airline passenger screening, are largely blinded because unreliable documents issued by the fifty states and the District of Columbia for non-security related purposes, for which a low level of reliability suffices, are now used for security purposes, which require a much greater degree of authenticity. Moreover, although driver's licenses are treated as de facto national ID cards—those issued by any one state are recognized by all others and by federal authorities—individual states continue to be in charge of issuing these licenses. Furthermore, each state continues to be free to follow its own procedures for verifying the identity of those who are awarded driver's licenses. The data presented below shows that many states continue to follow lax procedures.

In effect, the federal government has made the states into agents of national security, laying on them one more mandate without providing the means (budgets) or guidance (legislation) to allow them to carry out this new mission. Congress so far has offered only minimal financial support for the effort to improve the reliability of state driver's licenses. And draft bills calling for comprehensive measures to improve both the security of the issuance process and the cards themselves have not gained support from either the White House or Congressional leaders. The repercussions have clearly been detrimental to homeland protection.

The result is that future terrorists could readily acquire counterfeit or false means of identification, just as they did before September 11th. Several of the September 11th hijackers and

their associates have been found to have used counterfeit social security numbers that were never issued by the Social Security Administration (SSA). Meanwhile, one of the hijackers used the social security number of a child, and other hijackers used numbers that had been associated with multiple names.¹ This fake or counterfeit information seems to have been used by the hijackers to obtain driver's licenses. Some of the hijackers held multiple licenses from states including Virginia, Florida, California, Arizona, and Maryland. Only one of the hijackers appeared not to possess a state-issued form of ID, according to Senator Richard Durbin at his hearing on driver's licenses in April 2002.² (Timothy McVeigh also used a fake ID to rent the Ryder van that exploded in front of the Murrah Federal Building in Oklahoma City in April 1995.³)

II. A Report Card

1. All fifty states and the District of Columbia are currently unable to verify whether an applicant holds a driver's license in another state. Currently, the only database available to state DMV officials is the National Highway Traffic Safety Administration's (NHTSA) National Driver Register (NDR), which employs the Problem Driver Pointer System (PDPS) to determine whether an applicant has had a license revoked or suspended by another state. This registry does not, however, allow access to any information about applicants who have not had action taken against their licenses. As a result, there is no way to prevent a person from acquiring multiple licenses and ID cards from any number of states. Hence, an individual who is collaborating with terrorists could obtain several driver's licenses and share the "extras" with terrorists, without drawing notice to himself or to them.

2. 16 states have not implemented (and do not have plans to do so in the future) the Social Security Online Verification system (SSOLV)*, a service that allows DMV officials to instantly verify that a person is giving the correct social security number when he or she applies for a license, which in turn helps verify the person's identity.

The other way that states can verify social security numbers is through the “batch system,” by which DMV officials submit social security numbers in hard copy to the SSA to be verified. The batch system is particularly vulnerable. The GAO concluded last year that the SSA fails to inform DMVs when the social security number belongs to a deceased person after their agents were able to acquire licenses from two states that utilized batch matching.⁴ Furthermore, this process typically takes 24-48 hours, during which time several states issue driver's licenses to unverified applicants. If the DMVs receive a negative report from the SSA, they advise the license holder to clear the problem with the social security number they provided. If that is not done within a specified period, that person's file is flagged and then dealt with either upon renewal or if they request a duplicate card. However, law enforcement generally does not pursue those individuals who do not respond to requests to resolve the problem unless other facts warrant such action.

3. No standardization has been introduced with respect to the documents that a person must present to show that he or she is legally in the United States when applying for a driver's license. Each state has its own laws regarding what is required to prove “legal presence” (and some have no such laws at all [see below]). Some states may accept documents such as expired border crossing cards or letters from U.S. Customs and Immigration Services indicating that a person is

* Please refer to the section of this report entitled “A Note on Sources and Accuracy of the Data.”

in the process of achieving a certain status, which are much less reliable than visas or official Customs and Immigration documents. (This problem also exists for U.S. citizens. States accept different documents to verify the identity and residency of the person applying for a driver's license or state-issued identification card, and some states only require proof of identity. The acceptable documents may include utility bills, birth certificates, voter registration cards, notarized statements, Social Security cards, health insurance cards, hunting licenses, and school IDs. The varying state requirements create an environment in which people who seek to obtain false IDs seek out the state with the most lax requirements.)

4. Although this number is continuously in flux, 17 states currently do not require proof of legal presence, while still others do not require such proof during the license renewal process. (When the author of this report, Amitai Etzioni, himself an immigrant, had his driver's license renewed in the District of Columbia in 2004, he was not asked to produce any proof of legal presence, even though his previous driver's license was issued before September 11th and no such documentation was required at that time.)

5. In determining the expiration date for the driver's licenses of non-citizens, only 12 states have a policy of tying the expiration date of the license to that of the applicant's visa or legal "end of stay" documents. As a result, it is possible for non-citizens to have valid driver's licenses even after they are no longer legally in the United States.

6. Only 9 states are currently collecting biometric information, which is the most reliable means of identification, and only 8 are reporting that they plan to do so in the future. Many of the identifying features currently used in driver's licenses are not the most reliable; for instance, a person's eye color can be altered through the use of contact lenses, and weight often varies from

what is listed on the card. Furthermore, the wide availability of sophisticated graphic software programs and high-quality colored printers, as well as how-to books, make it easy to create counterfeit IDs. (Biometric technology is already required for foreigners' visas, and the State Department plans to use facial recognition technology in American passports in the future.) Furthermore, the states that do collect biometric information have many options to choose from, ranging from fingerprints to facial scans. Without a common standard, biometric information collected by one state is useless to another if they do not collect the same kind.

* * *

If one evaluates each state (as well as the District of Columbia) based on four basic criteria—whether the state uses SSOLV, whether it requires proof of legal presence, whether it ties the expiration of non-citizens' licenses to that of their visas or “end of stay” documents, and whether it collects biometric information—one can get a sense of the rigor of each state's current licensing procedures.

Three states deserve an A for their efforts to make driver's licenses more secure, having met all four criteria: Colorado, Kentucky, and West Virginia.

Fifteen states have met three of the criteria, and thus deserve a B: Arizona, California, Florida, Georgia, Illinois, Iowa, Mississippi, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, South Dakota, Virginia, and Wyoming. The District of Columbia also falls into this group.

Ten states have met two of the criteria, and are given a grade of C: Alabama, Idaho, Maine, Maryland, Massachusetts, Nevada, New Mexico, North Carolina, South Carolina, and Texas.

Eighteen states have met only one of the criteria, earning them a D: Arkansas, Connecticut, Delaware, Hawaii, Indiana, Kansas, Louisiana, Minnesota, Missouri, Montana, Nebraska, New Hampshire, North Dakota, Rhode Island, Tennessee, Utah, Vermont, and Washington.

Four states deserve an F for failing to meet any of the criteria: Alaska, Michigan, Oregon, and Wisconsin.

A state-by-state chart can be found on the following pages.

License to Hide: A State-by-State Report Card*

	Employ SSOLV	Legal Presence Requirement	Expiration of License tied to visa	Biometric Information Collected	Grade
Alabama	Y	Y	N	N	C
Alaska	N	N	N	N	F
Arizona	Y	Y	N	Plans to	B
Arkansas	N	Y	N	N	D
California	Y	Y	N	Plans to	B
Colorado	Y	Y	Y	Y	A
Connecticut	N	Y	N	N	D
Delaware	N	Y	N	N	D
DC	Y	Y	N	Y	B
Florida	Y	Y	Y	N	B
Georgia	Y	Y	N	Y	B
Hawaii	N	N	N	Y	D
Idaho	Y	Y	N	N	C
Illinois	Y	Y	N	Y	B
Indiana	N	Y	N	N	D
Iowa	N	Y	Y	Plans to	B
Kansas	N	Y	N	N	D
Kentucky	Y	Y	Y	Y	A
Louisiana	N	Y	N	N	D
Maine	Y	Y	N	N	C
Maryland	Y	Y	N	N	C
Massachussetts	Y	Y	N	N	C
Michigan	N	N	N	N	F
Minnesota	N	Y	N	N	D
Mississippi	Y	Y	N	Plans to	B
Missouri	Y	N	N	N	D
Montana	Y	N	N	N	D
Nebraska	Y	N	N	N	D
Nevada	Y	N	Y	N	C
New Hampshire	N	Y	N	N	D
New Jersey	Y	Y	N	Plans to	B
New Mexico	Y	N	N	Plans to	C
New York	Y	Y	N	Plans to	B
North Carolina	Y	N	N	Y	C
North Dakota	N	Y	N	N	D
Ohio	Y	Y	Y	N	B
Oklahoma	N	Y	Y	Plans to	B

Oregon	N	N	N	N	F
Pennsylvania	Y	Y	Y	N	B
Rhode Island	Y	N	N	N	D
South Carolina	Y	Y	N	N	C
South Dakota	Y	Y	Y	N	B
Tennessee	Y	N	N	N	D
Texas	Y	N	N	Y	C
Utah	Y	N	N	N	D
Vermont	Y	N	N	N	D
Virginia	Y	Y	Y	N	B
Washington	Y	N	N	N	D
West Virginia	Y	Y	Y	Y	A
Wisconsin	N	N	N	N	F
Wyoming	Y	Y	Y	N	B

* Please refer to "A Note on Sources and Accuracy of the Data"

III. A Note on Sources and Accuracy of the Data

In compiling this report, we relied on a 2004 survey of the motor vehicle departments of each state and the District of Columbia. Several states did not respond to our queries, despite repeated requests. In those cases, we relied on other sources of information, including reports from the American Association of Motor Vehicle Administrators (AAMVA), the GAO, and others. The report is a “snapshot” of regulations as they existed in our recent queries; state licensing policies often change.

In preparing this report, we also drew on a previous report issued by the Markle Task Force’s Subgroup on Reliable Identification for Homeland Protection and Collateral Gains.⁵

IV. Additional Evidence

Driver’s Licenses Abused at the Border

An investigation conducted by the GAO between September 2002 and May 2003 found that in every instance—without a single exception—when agents attempted to enter the United States from Western Hemisphere countries using counterfeit driver's licenses and birth certificates with fake identities they were successful. The border patrol agents failed to realize that the documents were not authentic. For the security tests, OSI agents used widely-available computer graphics software to create counterfeit documents; in other words, they used material that could be found in an average home.

In the course of this investigation, GAO agents used counterfeit documents and false identities to enter the United States from four countries. It is important to keep in mind that U.S. citizens—or people claiming to be U.S. citizens—seeking to enter the United States from Western Hemisphere countries are not required to show a passport to enter the United States;

instead, they are required to prove American citizenship. This may be done through a state-issued birth certificate or a baptismal record, and photo identification, for instance a driver's license, or, as the GAO notes, "since the law does not require that U.S. citizens who enter the United States from Western Hemisphere countries present documents to prove citizenship they are permitted to establish U.S. citizenship by oral statements alone."⁶ Teams of two GAO agents tried to enter the United States from Canada three times, from Mexico two times, from Jamaica one time, and from Barbados one time. Each time agents were able to cross the border—whether at an airport, a land border crossing, or a sea port of entry—and border patrol agents failed to recognize that the documents that the undercover agents were using were counterfeit.⁷

At Federal Buildings and Airports

In April and May of 2000, the GAO's OSI agents tried to gain access to nineteen federal buildings and two airports using counterfeit law enforcement credentials (that were either acquired from public sources or were created using commercial software packages, information from the Internet, and an ink-jet color printer). Agents gained entry into eighteen of the twenty-one sites on their first attempt; they entered the other three sites on their second attempt. Thus, at all sites the agents were successful and authorities did not detect the counterfeit documents. The facilities in which the agents gained entry were not minor ones, but rather included some of the most sensitive and, presumably, most secure facilities, such as the CIA, the Pentagon, the FBI, the Department of State, the Department of Justice, and others.⁸

Upon entering the "secure" buildings or the airport terminals, the undercover agents, carrying counterfeit credentials, declared that they were armed law enforcement officials and were able to pass through security without being screened." The GAO reported that at the 21

sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials," since one agent always carried a valise.⁹

Another troubling finding was that at fifteen of the sixteen facilities where agency heads or cabinet secretaries worked, agents were able to stand directly outside their suites. The five times agents attempted to enter the suites, they were able to do so successfully. Undercover agents also were able to enter restrooms near the agency head's or cabinet secretary's suite and could have left dangerous materials there without being detected.¹⁰

Airport officials did not detect the counterfeit documents either. Airline ticket agents readily gave the undercover GAO agents "law enforcement" boarding passes. Although the procedures for getting through security varied at the two airports, none of the agents nor their valises were screened by security personnel.¹¹

In response to these findings, nineteen of the twenty-one agencies and airports that were part of the original GAO study responded that they had taken specific actions to enhance their security in the wake of the findings.¹² However, since then a task force investigation into Washington, D.C. area airports immediately following September 11, 2001 revealed that those airports' general security system remains lax. The task force, formed by U.S. Attorney Paul McNulty of the Eastern District of Virginia, examined the records of airport employees who held Security Identification Display Area badges, which allow access to secured areas of Dulles International and Reagan National Airports.¹³ McNulty reported to the House of Representatives that the investigation found that "75 airport workers used false or fictitious social security account numbers to obtain security badges and that afforded them unescorted access into the

most sensitive areas of our airports."¹⁴ He went on to say that "Many of these airport workers also used the same false or fictitious social security number to obtain Virginia driver's licenses, fill out immigration forms, or apply for credit cards."¹⁵

The Washington area airports were not alone in having individuals use fraudulent identifiers to obtain security passes. After the September 11th terrorist attacks, a Department of Justice investigation into employees at the Salt Lake City International Airport found that "61 individuals with the highest-level security badges and 125 with lower level badges. . . misused SSN's" to obtain security badges or fill out employment eligibility forms.¹⁶

On the Not-So-Black Market

Raids in the Seattle area in September 2002 netted enough computer equipment and specialty paper to print more than eight hundred fraudulent documents, including driver's licenses, Social Security cards, green cards, and Mexican driver's licenses.¹⁷ In Washington, D.C., raids resulting from an ongoing investigation which began in April, 2002 have netted more than one thousand fraudulent documents and nearly fifty arrests.¹⁸ In one bust during this ongoing investigation, authorities confiscated more than five hundred fake residency cards, Social Security cards, driver's licenses, and other IDs at a single residence.

And on the Internet

The increasingly widespread use of the Internet to obtain false identification materials also poses problems for reliable means of identification, especially driver's licenses. David C. Myers, coordinator of the Fraudulent Identification Investigation Program for the Florida Division of Alcoholic Beverages and Tobacco, reported to the Senate in May 2000 that "about 30 percent of the false identification cards I see come from the Internet" and that "some false ID

sites have received over 10,000 inquiries on a single day."¹⁹ This is not that surprising given that Myers also testified that many high-quality ID cards can be purchased on the Internet for anywhere between \$30 and \$300.²⁰ Thus, many underage college students, and certainly individuals with more nefarious plans, look to web sites like www.phonyid.com and www.novelty-ids.com to help them obtain fake IDs.

More recently, in September 2003 John S. Pistole, acting assistant director of the FBI's Counterterrorism Division, discussed the pervasiveness of false means of identification. In his testimony before the Senate he said that it is not that false means of identification are new to law enforcement, but rather that the pervasiveness of the false means is new. The Internet and our technological sophistication—especially in terms of computer programs and printers—have made it so easy to produce high quality documents that "nearly anyone can be an expert."²¹ Pistole also pointed out that, "The tremendous growth of the Internet, the accessibility it provides to such an immense audience coupled with the anonymity it allows result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme."²²

V. Remedies

The federal government should conduct research on affordable methods of improving identification systems and making the entire identification mechanism more verifiable. The research should devote due attention to concerns about privacy and civil liberties. The government should encourage states to implement the studies' findings and adopt interstate standards, and to implement them through the use of federal grants.

In each jurisdiction the fines and penalties for individuals who possess, attempt to obtain, or sell counterfeit or false identification should be increased, as should the fines and penalties for

individuals who knowingly supply such identification or knowingly allow people with such false or counterfeit means of identification to enter controlled areas. These penalties should be part of federal, and not merely state, law.

Specifically

- The federal government should provide states with assistance in making state driver's licenses and other state-issued identification cards more reliable as quickly as possible because they are the most widely used form of identification in the United States.
 - *Process Remedies*
 - Paper breeder documents should be standardized.
 - Birth and death certificate records should be should be digitized and searchable in all states. One existing program that addresses this need and therefore deserves further support is the E-Vital program, which establishes a common process through which birth and death record information can be analyzed, processed, collected, and verified. The owner of these data should have privacy protection measures in place which address issues such as who may access the data and for what purposes, as well as have enforcement policies. For instance, to protect civil liberties, audit trails should be established.
 - States should verify that the social security number a person presents when applying for a driver's license is not someone else's only through the SSOLV system. The Department of

Transportation should provide the needed funds so states will be encouraged to undertake this verification step. It is estimated that implementing SSOLV in the remaining states would cost \$4.2 million.

- Federal legislation should tie the expiration date of the driver's license or other state-issued identification card to the expiration date of the foreign visitor's visa, as some states are already doing.
- State driver's licenses should meet minimum uniform standards concerning the data content and the verifiability of the credential.
- Congress should pass legislation requiring state motor vehicle agencies to only accept a limited set of approved documents to prove identity and residency.
- State motor vehicle databases should be integrated for ordinary drivers. (Such integration of databases has already been undertaken for those who hold commercial driver's licenses. The program, called the Commercial Driver's License Information System [CDLIS], was designed to make sure that commercial drivers only possess one driver's license and do not simultaneously carry licenses from more than one state. The program, mandated by the Commercial Vehicle Safety Act of 1986, has been in effect since 1992; and it has kept 871,000 individuals from obtaining licenses, according to the AAMVA.) Congress should mandate a program,

similar to the Commercial Driver's License Information System, for all driver's license holders to ensure that an individual only holds one license from one state at a given time. Such a program could be completed for about \$80 million.

- *Personnel Remedies*
 - State motor vehicle agencies should provide their employees with ongoing, detailed training about how to spot counterfeit or false documents and should provide law enforcement personnel with guidelines for how to check the validity of driver's licenses.
 - They should also launch aggressive oversight, auditing, and anti-corruption policies to help prevent fraud and make it easier to detect fraud when it occurs in the driver's license issuing process.
- *Technology Remedies*
 - The federal government should dedicate resources to determining whether biometric and cryptographic technologies may be used to make driver's licenses and other forms of identification more reliable and determining which technology, if any, is appropriate and how the technology and enrollment processes may be implemented (including which technologies may be used, e.g., smart cards, two-dimensional bar codes, scanners for network verification, magnetic stripes, etc.), given the primary purposes and uses of these means of identification.

- The card's electronic code—magnetic strips, smart chips, whatever the uniform mean may be—should be encrypted and should contain all the information already on the driver's license.
- Reliable means of identification should work both online and offline. Introducing a much higher level of security in one but not the other will greatly undermine security because it will invite those who seek to attack us to focus on the less-covered front.
- To combat the explosive growth of false identification on the Internet, federal authorities, in particular, the Secret Service, which enforces laws involving counterfeit and fraudulent identification, should be given resources to shut down web sites in the United States that issue false or counterfeit IDs. Furthermore, Congress should pass legislation that would require servers to collaborate in tracing and shutting down web sites that issue fraudulent or counterfeit identification.

Privacy Protection and Accountability

It is important to note that the more reliable means of identification are—the better privacy is protected. The reason for this is that if these means are unreliable, security commands collecting more information about the person in order to help locate and identify him or her. To that end:

- Concerns about privacy should be addressed in all matters concerning more reliable means of identification. Studies of new

ways to make means of identification more reliable should also include new ways to protect privacy and other civil liberties.

- For personal data such as digitized birth and death certificate records, those who hold the data should have privacy protection measures in place which address issues such as who may access the data and for what purposes, as well as have enforcement policies. For instance, audit trails, which could detect unauthorized use of data and thus help deter it, should be established.
- The Department of Homeland Security should set up a public-private body to review more reliable means of identification measures which are used for homeland security purposes as they emerge and also to examine the measures' effectiveness and privacy implications. This body should operate under the criteria specified in the Federal Advisory Committee Act.

The AAMVA correctly points out that a piecemeal approach – fixing one, two, or even several of the elements – will not suffice. To that end, the AAMVA has developed a comprehensive approach, which incorporates many of the remedies listed here, as well as some others. Taken together, they provide a systematic approach to the subject. However, the necessary resources – and legal framework (above all for minimal standardization) – will have to come from the federal government.

Endnotes

-
1. Prepared Testimony of James G. Huse, Jr., Inspector General, Social Security Administration, before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security and Subcommittee on Immigration, Border Security, and Claims, 107th Cong., 2nd Sess., 25 June 2002.

 2. Statement of Senator Richard Durbin before the Senate Governmental Affairs Subcommittee on Restructuring and the District of Columbia Subcommittee and Subcommittee on Oversight of Government Management on Fake or Fraudulently Issued Driver's Licenses, 107th Cong., 2nd Sess., 16 April 2002.

 3. Statement of Senator Richard Durbin before the Senate Governmental Affairs Subcommittee on Restructuring and the District of Columbia Subcommittee and Subcommittee on Oversight of Government Management on Fake or Fraudulently Issued Driver's Licenses, 107th Cong., 2nd Sess., 16 April 2002.

 4. House Ways and Means Committee, "GAO Reveals Driver License Vulnerability to Identity Thieves," 24 September 2003, available at <http://waysandmeans.house.gov/News.asp?FormMode=print&ID=125>.

 5. Subcommittee on Reliable Identification for Homeland Protection and Collateral Gains, "Reliable Identification for Homeland Security and Collateral Gains," *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force* (New York: Markle Foundation, December 2003): Appendix A.

6. Prepared Testimony of Robert J. Cramer, Managing Director, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Immigration, Border Security, and Claims on Counterfeit Documents Used to Enter the United States From Certain Western Hemisphere Countries Not Detected, 108th Cong., 1st Sess., 13 May 2003 (GAO-03-713T).

7. Prepared Testimony of Robert J. Cramer, Managing Director, Office of Special Investigations, General Accounting Office, before the Senate Committee on Finance on Weaknesses in Screening Entrants Into the United States, 108th Cong., 1st Sess., 30 January 2003 (GAO-03-438T); and Prepared Testimony of Robert J. Cramer, Managing Director, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Immigration, Border Security, and Claims on Counterfeit Documents Used to Enter the United States From Certain Western Hemisphere Countries Not Detected, 108th Cong., 1st Sess., 13 May 2003 (GAO-03-713T).

8. Prepared Testimony of Robert H. Hast, Assistant Comptroller General for Investigations, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Crime on Breaches at Federal Agencies and Airports, 106th Cong., 2nd Sess., 25 May 2000 (GAO/T-OSI-00-10).

9. Prepared Testimony of Robert H. Hast, Assistant Comptroller General for Investigations, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Crime on Breaches at Federal Agencies and Airports, 106th Cong., 2nd Sess., 25 May 2000 (GAO/T-OSI-00-10).

10. Prepared Testimony of Robert H. Hast, Assistant Comptroller General for Investigations, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Crime on Breaches at Federal Agencies and Airports, 106th Cong., 2nd Sess., 25 May 2000 (GAO/T-OSI-00-10).

11. Prepared Testimony of Robert H. Hast, Assistant Comptroller General for Investigations, Office of Special Investigations, General Accounting Office, before the House Judiciary Subcommittee on Crime on Breaches at Federal Agencies and Airports, 106th Cong., 2nd Sess., 25 May 2000 (GAO/T-OSI-00-10); and Letter from Robert H. Hast, Managing Director, Office of Special Investigations, General Accounting Office, to the Honorable Lamar Smith, Chairman of House Judiciary Subcommittee on Crime regarding Security Improvement Inquiry, 31 August 2001 (GAO-01-1069R).

12. Letter from Robert H. Hast, Managing Director, Office of Special Investigations, General Accounting Office, to the Honorable Lamar Smith, Chairman of House Judiciary Subcommittee on Crime regarding Security Improvement Inquiry, 31 August 2001 (GAO-01-1069R). One agency, the CIA, did not provide a specific response to the inquiry and the other agency, the U.S. Courthouse and Federal Building in Orlando, Florida was not part of the follow-up. However, the GAO reports it contacted the U.S. Marshals Service and the General Services Administration, which are responsible for the security of judicial facilities and federal buildings.

13. Department of Justice Press Release, "Attorney General Statement Regarding Airport Security Initiative," 23 April 2002. Available at:
http://www.usdoj.gov/opa/pr/2002/April/02_ag_246.htm. Accessed 25/6/03.

14. Prepared Testimony of Paul J. McNulty, U.S. Attorney for the Eastern District of Virginia, before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security and Claims, 107th Cong., 2nd Sess., 25 June 2002.

15. Prepared Testimony of Paul J. McNulty, U.S. Attorney for the Eastern District of Virginia, before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security and Claims, 107th Cong., 2nd Sess., 25 June 2002.

16. Office of the Inspector General, Social Security Administration, *Social Security Number Integrity: An Important Link in Homeland Security*, Management Advisory Report, May 2002 (A-08-02-22077).

17. Diane Brooks, "Raids Net Pile of Fake IDs," *Seattle Times*, 14 September 2002, B1.

18. Warren A. Lewis (Interim Director, Washington District Office, Bureau of Immigration and Customs Enforcement, Department of Homeland Security), Letter to the Editor, *Washington Post*, 17 May 2003, A24.

19. Prepared Testimony of David C. Myers, Special Agent, Identification Fraud Coordinator, Florida Division of Alcoholic Beverages and Tobacco, Department of Business and Professional Regulation, Fraudulent Identification Unit, before the Senate Governmental Affairs Permanent Subcommittee on Investigations on Phony IDs and Credentials Via the Internet, 106th Cong., 2nd Sess., 19 May 2000.

20. Prepared Testimony of David C. Myers, Special Agent, Identification Fraud Coordinator, Florida Division of Alcoholic Beverages and Tobacco, Department of Business and Professional Regulation, Fraudulent Identification Unit, before the Senate Governmental Affairs Permanent Subcommittee on Investigations on Phony IDs and Credentials Via the Internet, 106th Cong., 2nd Sess., 19 May 2000.

21. Prepared Testimony of John S. Pistole, Acting Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, before the Senate Finance Committee on Homeland Security and Terrorism Threat From Document Fraud, Identity Theft and Social Security Number Misuse, 108th Cong., 1st Sess., 9 September 2003.

22. Prepared Testimony of John S. Pistole, Acting Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, before the Senate Finance Committee on Homeland Security and Terrorism Threat From Document Fraud, Identity Theft and Social Security Number Misuse, 108th Cong., 1st Sess., 9 September 2003.