United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2012

DRIVER'S LICENSE SECURITY

Federal Leadership Needed to Address Remaining Vulnerabilities

GAO-12-893

September 2012

DRIVER'S LICENSE SECURITY

Federal Leadership Needed to Address Remaining Vulnerabilities

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-893, a report to congressional requesters.

Why GAO Did This Study

Obtaining a driver's license under another's identity can enable criminals to commit various crimes. The 9/11 terrorists, for example, possessed fraudulent licenses. The REAL ID Act sets minimum standards for states when verifying license applicants' identity, which go into effect in January 2013. If states do not meet these requirements, their licenses will not be accepted for official purposes such as boarding commercial aircraft. DHS is responsible for establishing how states may certify compliance and for determining compliance. SSA helps states verify SSNs. GAO was asked to examine (1) states' identity verification procedures for license applicants, (2) the procedures' effectiveness in addressing fraud, and (3) how federal agencies have helped states enhance procedures. GAO analyzed DHS and SSA data on states' use of verification systems; interviewed officials from DHS, SSA, and other organizations; and conducted on-site or phone interviews with licensing agency officials in 11 states. GAO tested state procedures in three states that have known vulnerabilities; results from these states are not generalizable.

What GAO Recommends

GAO recommends that DHS work with partners to take interim actions to help states address cross-state and birth certificate fraud. DHS did not concur with these recommendations, saying its ongoing efforts are sufficient. GAO has demonstrated that vulnerabilities remain as long as national systems are not yet fully operational. Therefore, GAO continues to believe additional DHS actions are needed.

View GAO-12-893. For more information, contact Daniel Bertoni at (202) 512-7215 or bertonid@gao.gov.

What GAO Found

To verify license applicants' identity, all 50 states and the District of Columbia have procedures that may detect counterfeit documents. For example, all states are now verifying key personal information, such as Social Security numbers (SSN) through online queries to a Social Security Administration (SSA) database, a significant increase from about a decade ago. This effort helps ensure that the identity information presented belongs to a valid identity and also is not associated with a deceased person. Additionally, most states verify non-citizen applicants' immigration documents with the Department of Homeland Security (DHS) to ensure these individuals have lawful status in the United States. Many states are also using facial recognition techniques to better detect attempts to obtain a license under another's identity. While most states have taken steps required by the REAL ID Act of 2005 (Act), officials in some states indicated that they may not comply with certain provisions—such as re-verifying SSNs for license renewals—because of state laws or concerns that these requirements are unnecessary and burdensome.

State officials interviewed by GAO report that identity verification procedures have been effective at combating certain kinds of fraud, but vulnerabilities remain. Officials in most of the 11 states GAO contacted reported a decline in the use of counterfeit identity documents, and officials in states using facial recognition said they detected a number of identity theft attempts. However, criminals can still steal the identity of someone in one state and use it to get a license in another because states lack the capacity to consistently detect such cross-state fraud. A system for addressing such fraud would enable states to comply with the Act's prohibition against issuing licenses to individuals who already have a license from another state, but may not be fully operational until 2023. Furthermore, officials in many states said they have difficulties detecting forged birth certificates. Verifying date of birth is also required by the Act, and a system exists for doing so, but no licensing agencies are using it because of concerns about incomplete data, among other reasons. Partly because these two systems are not fully operational, GAO investigators were able to use counterfeit out-of-state drivers' licenses and birth certificates to fraudulently obtain licenses in three states.

By improving their respective verification systems, SSA and DHS have helped states enhance their identity verification procedures. For example, SSA has established timeliness goals for responding to state SSN queries and DHS has addressed data accuracy issues. DHS has also provided funding for states to develop new systems. However, DHS has not always provided timely, comprehensive, or proactive guidance to help states implement provisions of the Act related to identity verification. For example, DHS did not issue formal, written guidance in this area for more than 4 years after issuing final regulations, even though officials from most states GAO interviewed said they needed such guidance. Additionally, even though relevant national systems are not yet fully operational, DHS has no plans to promote certain alternatives states can use to comply with the Act's identity verification requirements and combat cross-state and birth certificate fraud. Officials in some states indicated they needed direction from DHS in this area.

Contents

Abbreviations

AAMVA	American Association of Motor Vehicle Administrators
DHS	Department of Homeland Security
DLSGP	Driver's License Security Grant Program
EVVE	Electronic Verification of Vital Events
FTC	Federal Trade Commission
HHS	Department of Health and Human Services
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
NAPHSIS	National Association for Public Health Statistics and Information Systems
NIST	National Institute of Standards and Technology
PDPS	Problem Driver Pointer System
SAVE	Systematic Alien Verification for Entitlements
SSA	Social Security Administration
SSN	Social Security number
SSOLV	Social Security Online Verification
VLS	Verification of Lawful Status

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 21, 2012

The Honorable Sam Johnson, Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

The Honorable Candice S. Miller, Chairman
Subcommittee on Border and Maritime Security
Committee on Homeland Security
House of Representatives

Driver's license fraud is a crime that can have significant financial and domestic security consequences. Because drivers' licenses have become a widely accepted form of identification, identity thieves may try to obtain a license under someone else's name—with forged or stolen Social Security cards or other documents—and use it to commit financial fraud. By one estimate, in 2010 over 8 million Americans were victims of identity theft and such crimes cost victims a total of $37 billion.[1] Individuals may also try to obtain licenses for other criminal purposes; for example, some of the 9/11 terrorists obtained licenses fraudulently. In 2005, after the National Commission on Terrorist Attacks Upon the United States recommended enhanced security for licenses, Congress passed the REAL ID Act of 2005 (REAL ID Act or Act), which, among other provisions, sets minimum national standards for driver's license security including procedures for states to follow when verifying the identity of license applicants.[2] States have until January 2013 to comply with the Act's requirements. While states are not required to comply, if they choose not to, the licenses they issue will no longer be accepted for official purposes as defined in the Act, such as boarding commercial aircraft.

We were asked to review the current status of states' identity verification procedures when issuing drivers' licenses, such as those related to Social

[1]Congressional Research Service, *Identity Theft: Trends and Issues,* R40599 (Washington, D.C.: Dec. 14, 2011).

[2]Pub. L. No. 109-13, div. B, 199 Stat. 231, 302. Title II of the REAL ID Act addresses driver's license security and is codified at 49 U.S.C. § 30301 note.

Security number (SSN) verification. Specifically, we address: (1) what procedures states have in place to verify the identity of driver's license applicants, (2) how effective these procedures have been in addressing license application fraud and what vulnerabilities remain, and (3) what actions federal agencies have taken to help states enhance their identity verification procedures. In addressing these objectives, we focused solely on procedures for verifying license applicants' identity and did not review other aspects of driver's license security that are addressed by Title II of the REAL ID Act. We reviewed relevant federal laws and regulations, selected state laws, and previous studies. We interviewed officials from two federal agencies that have a role in helping states implement the Act: the Department of Homeland Security (DHS) and the Social Security Administration (SSA). We collected and analyzed national data from SSA and DHS on states' use of verification systems, and performed a data reliability assessment—including a review of related documentation and interviews with agency officials—that determined the data were sufficiently reliable for reporting the number of states using these systems and the verification rates they obtained. We also interviewed officials from a number of other organizations, including the American Association of Motor Vehicle Administrators (AAMVA), which represents and provides guidance to state licensing agencies; the National Association for Public Health Statistics and Information Systems (NAPHSIS), which represents the vital records agencies that issue birth certificates; the Coalition for a Secure Driver's License; the Center for Immigration Studies; and the National Governors Association. To gain a more in-depth perspective on identity verification procedures and their impact at the state level, we conducted site visits to three states (Iowa, New York, and Texas). During the site visits, we interviewed officials at the state licensing agency headquarters and local license issuance branches, including investigative staff. We also conducted phone interviews with driver licensing agencies in eight additional states (California, Florida, Maryland, Minnesota, New Hampshire, Ohio, Pennsylvania, and Washington). In three of our states we also interviewed officials with vital records agencies, which issue birth certificates. We judgmentally selected states based on factors including geographical dispersion, population, and use of particular identity verification procedures. While our review of procedures in these 11 states cannot be generalized to all states, in 2010 these states represented almost half of the U.S. population. Finally, our investigative staff tested identity verification procedures by attempting to obtain licenses under fictitious identities in three states. We chose states with certain identified vulnerabilities in their procedures. The results from these three states cannot be generalized to others.

We conducted this performance audit from September 2011 through September 2012 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We performed our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

Drivers' licenses have become widely accepted as an identity document because they generally contain identifying information such as the licensee's name, photograph, physical description, and signature and may include features that make them more difficult to counterfeit or alter. As of 2010, about 210 million drivers were licensed in the United States.[3] Due to the crucial role of the driver's license as an identity document, individuals may try to fraudulently obtain them for a wide range of purposes. For example, some may try to get a license in someone else's name to commit financial fraud, such as stealing government benefits, opening bank or credit card accounts, and writing counterfeit checks. Criminals may also obtain multiple licenses under different identities so they can commit criminal acts and, if apprehended, avoid having charges associated with their true identity. Illegal aliens may use a counterfeit license to live in the United States.

The prevalence of driver's license fraud in the United States is difficult to fully determine or quantify. The Federal Bureau of Investigation collects data from all states on a number of different categories of crimes through its Uniform Crime Reporting program, but this program does not have a category specifically for driver's license fraud. Estimates are, however, available from a few sources. For example, in 2010 the Federal Trade Commission (FTC) reported that complaints involving the issuance or forging of drivers' licenses accounted for 0.9 percent of the approximately 251,000 identity theft complaints it received overall (about 2,300

[3]Identification cards are issued for the sole purpose of identifying the owner and generally contain the same information as drivers' licenses but lack information authorizing the owner to drive. According to AAMVA, nationwide data are not readily available on the number of identification cards issued by states, as states do not consistently track this information.

complaints). Some evidence suggests, though, that many identity theft cases go unreported and thus the total number of identity theft cases may be substantially higher than the FTC figure. In addition, the Center for Identity Management and Information Protection analyzed 517 identity theft cases investigated by the U.S. Secret Service between 2000 and 2006, and found that counterfeit drivers' licenses were used in 35 percent of these cases.

Verifying license applicants' identity and preventing fraud has traditionally been a state responsibility, but after the terrorist attacks of September 11, 2001, there was an increased federal interest in driver's license issuance and security, as evidenced by the passage of the REAL ID Act of 2005. States are not mandated to comply with the Act; however, the Act establishes specific procedures states must follow when issuing drivers' licenses in order for those licenses to be accepted by federal agencies for "official purposes," including, but not limited to, boarding commercial aircraft, entering federal buildings, and entering nuclear power plants.[4,5] As of July 2012, 17 states had enacted laws expressly opposing implementation or prohibiting the relevant state agencies from complying with the REAL ID Act.[6] Under the REAL ID Act, DHS has primary responsibility for establishing how and when states can certify their compliance and determining whether states are compliant. DHS issued regulations in 2008 that provided details on how it would determine whether states were REAL ID-compliant.[7] Although the Act set a May 11, 2008, deadline for compliance, DHS' regulations allowed states to request an extension of the full compliance deadline to May 11, 2011, and

[4]49 U.S.C. § 30301 note. These requirements also apply to identification cards.

[5]The provisions of Title II of the REAL ID Act apply to the 50 states, the District of Columbia, and any U.S. territory or possession.

[6]These states are Alaska, Arizona, Georgia, Idaho, Louisiana, Maine, Minnesota, Missouri, Montana, New Hampshire, Oklahoma, Oregon, Pennsylvania, South Carolina, Utah, Virginia, and Washington. This list does not include states that may have passed legislative resolutions. According to an official from the National Conference of State Legislatures, many of these state laws are broadly written, and although they may prevent the state from becoming certified as REAL ID compliant, they do not necessarily bar states from complying with specific provisions of the REAL ID Act.

[7]73 Fed. Reg. 5272 (Jan. 29, 2008), codified as amended at 6 C.F.R. §§ 37.1 – 37.73.

the agency later pushed the date back to January 15, 2013.[8] If states are interested in complying with the Act, they must submit documentation no later than 90 days before this deadline (around October 15, 2012). Initially, after the January deadline, individuals with licenses from states determined to be compliant may continue to use their licenses for official purposes, regardless of when these licenses were issued, according to DHS. However, by December 1, 2014, certain individuals—those born after December 1, 1964—must be issued new, REAL ID-compliant licenses by states that have been determined to be compliant in order to use their licenses for official purposes. By December 1, 2017, all license holders must be issued new, REAL ID-compliant licenses in order to use them for official purposes.[9]

The REAL ID Act sets minimum standards for several aspects of the license and identification card issuance process.[10] In the area of identity verification, the Act establishes the following requirements, among others, for states seeking compliance:

- **Documentation:** States must require license applicants to provide documentation of their name, date of birth, SSN, address of principal residence, and lawful status in the United States;[11]

[8]DHS extended this deadline using its authority under section 205(b) of the Act to grant extensions to states. 73 Fed. Reg. 5272 (Jan. 29, 2008), 76 Fed. Reg. 12,269 (March 7, 2011).

[9]6 C.F.R. §§ 37.5, 37.51(a).

[10]In addition to identity verification requirements, Title II of the REAL ID Act also establishes requirements for other areas of the license issuance process. For example, it specifies the minimum information that must be displayed on licenses and requires that licenses include physical security features designed to prevent counterfeiting. Also, it requires states to ensure the physical security of the locations where licenses are produced and requires that anyone involved in the manufacturing of licenses be subject to an appropriate security clearance process.

[11]As defined in the REAL ID Act, individuals who have lawful status in the United States include, for example, U.S. citizens and nationals, aliens lawfully admitted for permanent or temporary residence, individuals with an approved or pending application for asylum or who entered the United States as refugees, and individuals with a valid nonimmigrant status. Certain individuals, such as those with nonimmigrant status or pending applications for asylum, may only be issued temporary licenses for periods no longer than their authorized stays in the country, or if there is no definite end to the period of authorized stay, a period of 1 year.

- **Verification:** Requires states to verify with the issuing agency the issuance, validity, and completeness of the documents presented as proof of name, date of birth, SSN (or verify the applicant's ineligibility for an SSN), address, and lawful status, with specific requirements to confirm SSNs with SSA and verify lawful status of non-citizens through an electronic DHS system;[12]
- **Image capture:** Requires states to capture and store digital images of all documents presented by license applicants to establish identity, such as passports and birth certificates, and capture the facial images of all applicants;
- **Renewals:** Requires states to establish an effective procedure for confirming or verifying the information provided by individuals seeking to renew their licenses;
- **One driver, one license:** Requires states to refuse to issue a license to an applicant who already holds a license from another state, without confirming that this other license has been or is in the process of being terminated; and
- **Staff training:** States must establish training programs on recognizing fraudulent documents for appropriate employees involved in issuing licenses.

States Have Taken Steps to Detect Counterfeit Documents and Identity Theft, Including Many Required by the REAL ID Act

State driver licensing agencies use a combination of different techniques to verify the identity of license applicants and prevent fraud. These various procedures are used together to detect license fraud and no single technique is sufficient, according to officials at several licensing agencies. All states have in place some procedures to detect counterfeit documents, which may include electronic systems to verify data contained on documents—such as the Social Security card—or visual inspection of documents. Many states also use other techniques to detect fraud, including facial recognition, cross-state checks, or internal controls for licensing transactions. (See table 1.)

[12]If a license applicant's SSN is already registered or associated with another individual who has already been issued a driver's license by any state, then this discrepancy must be resolved and appropriate action taken.

Table 1: Overview of State Licensing Agencies' Identity Verification Techniques

Technique	Purpose	Number of states using
Social Security Online Verification (SSOLV)	Ensure license applicant's SSN and other information is associated with a real person, not a fictitious identity or the identity of a deceased person	50 plus District of Columbia
Systematic Alien Verification for Entitlements (SAVE)	Ensure non-citizen applicant has lawful status in the United States	42 plus District of Columbia have agreements with DHS to use
Document inspection	Ensure applicant's identity documents are not forgeries	11 of 11 interviewed
Facial recognition and other biometric techniques	Ensure applicant does not obtain a license by using the identity of another individual and has not previously obtained licenses using a different identity or identities	41 plus District of Columbia
Cross-state photo-sharing	If an out-of-state license is presented, ensure it is authentic and belongs to applicant who presents it	23 plus District of Columbia
Internal control procedures	Prevent fraud by licensing agency employees	11 of 11 interviewed

Source: GAO analysis of data from SSA, DHS, and AAMVA, as well as interviews with state officials.

Electronic Verification Systems

All states plus the District of Columbia are now using Social Security Online Verification (SSOLV) to verify license applicants' SSNs and other personal data, consistent with the REAL ID Act's requirement to confirm SSNs with SSA. The number of states verifying SSNs with SSA has increased substantially since 2003, when we reported that 25 states were doing so.[13] Even states with laws opposing implementation of the REAL ID Act are checking SSNs through SSOLV. Use of SSOLV allows states to verify that the SSN provided by a license applicant is valid. In other words, SSOLV allows states to check whether (1) someone has been issued this SSN, (2) the SSN matches the name and date of birth provided by the applicant, and (3) the SSN is associated with a deceased

[13]See GAO, *Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, GAO-03-920 (Washington, D.C.: September 15, 2003). We reported that 25 states used either the online method—now known as SSOLV—or a separate batch method of verifying SSNs. The online method enables states to submit online requests to verify individual SSNs, with SSA providing immediate responses. In the batch approach, states submit an aggregate group of SSNs for verification and typically receive a response from SSA within 1 – 2 days. According to SSA, licensing agencies in three states continue to use the batch method for verifying some SSNs while also using SSOLV.

individual. Officials in most of the states we interviewed said they never or rarely issue a permanent driver's license before obtaining a verification of the applicant's personal data.[14] In fiscal year 2011, the SSOLV verification rate—that is, the percentage of SSOLV verification requests that confirmed the validity of the personal data submitted—was 93 percent on average nationwide, and almost all the states had rates above 85 percent. The national average is an increase from the 89 percent average rate in fiscal year 2008, the earliest year for which data were available. Officials in almost all of the states we interviewed said they had no concerns about the percentage of SSOLV queries that failed to verify. The most common reason for non-verifications nationwide in 2011 was that the name presented by the applicant did not match the name associated with the SSN on file with SSA. Officials in most of the states we interviewed cited name changes as the most common reason for this. A license applicant may have changed their name after marriage, but not reported this change to SSA. In such cases, states may ask applicants to resolve the issue with SSA and then return to the licensing agency so the SSOLV query may be run again.

Most states are also using Systematic Alien Verification for Entitlements (SAVE), another REAL ID Act requirement, but officials in some of the states we interviewed reported challenges with the system. SAVE, operated by DHS, verifies the information in documents that non-citizen applicants provide to prove they have lawful status in the United States. As of 2012, licensing agencies in 42 states plus the District of Columbia had agreements with DHS to use it.[15] However, a few states with such agreements do not use the system consistently for each non-citizen applicant. For example, officials in one state we interviewed said they used SAVE only when the documents submitted by a non-citizen raised questions, such as if they appeared tampered with or indicated a non-citizen no longer has lawful status in the country. Officials in the five

[14]Some states may issue licenses without obtaining a SSOLV verification on the applicant's personal data. For example, officials in one state said they may do so if the applicant provides documentation that their name was changed due to marriage. In that case, the submitted name is correct even though it does not verify the SSN in SSOLV. Officials in a few states said they may issue temporary licenses for use while a SSOLV non-verification is resolved.

[15]In addition, driver licensing agencies in American Samoa, the U.S. Virgin Islands, Guam, the Northern Mariana Islands, and Puerto Rico have entered into agreements with DHS to use SAVE. According to DHS, however, because American Samoa has an independent immigration framework it is not able to actually use SAVE to verify lawful status.

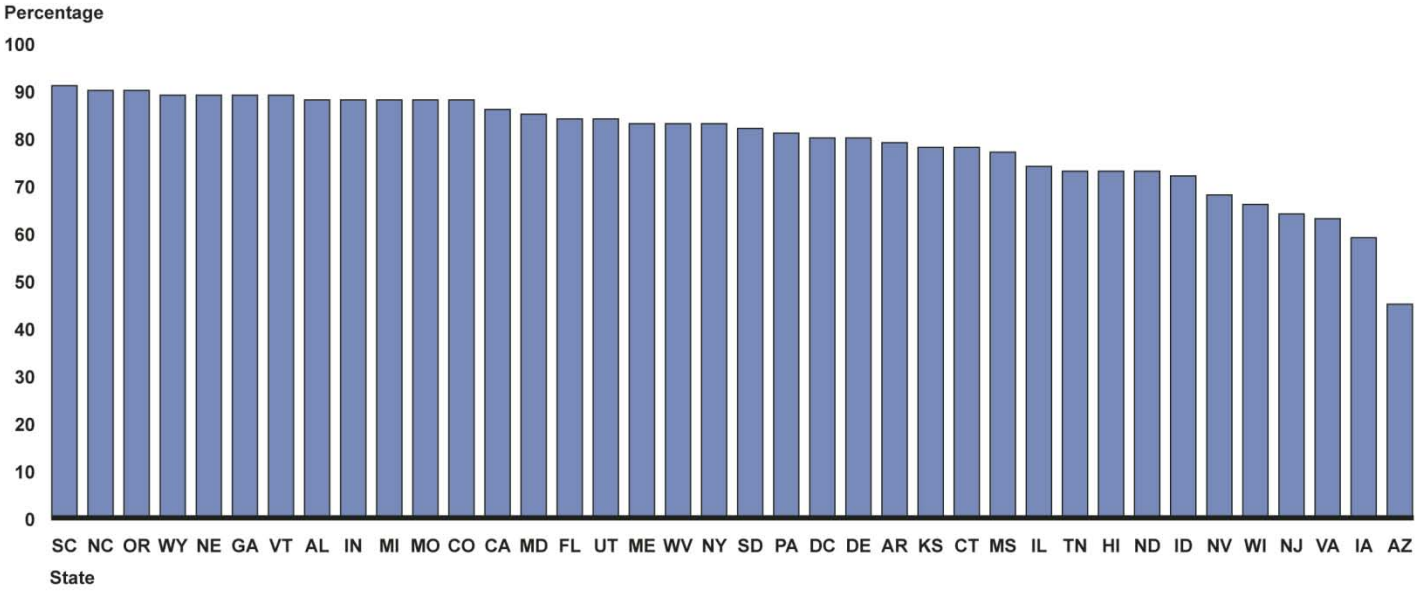
states we interviewed that were not using SAVE most often cited technological challenges, such as difficulties providing front-counter staff in local issuance branches with routine access to the system. Officials in all but one of these states said they plan to start using the system if these issues are resolved.

Officials in half of the states we interviewed that were using SAVE said they were concerned about the verification rate they obtained. When states submit data from non-citizens' lawful status documents, the system searches a variety of DHS databases in an effort to verify these data.[16] If data are not verified on the first attempt, the state may initiate a second and then a third attempt, which entail manual checks by DHS staff and additional costs for the state.[17] Officials in one state, for example, told us when SAVE does not verify lawful status on the first attempt, moving on to additional attempts requires additional efforts by staff. Officials in a few states said they believe data entry errors and delays in updating the data in DHS databases are common reasons that data are not verified; DHS officials also listed these as possible factors. Among all licensing agencies using SAVE, the verification rate for initial SAVE queries during fiscal year 2011 varied from 45 percent to 91 percent, according to DHS data (see fig. 1). DHS officials said it is possible that states that only submit SAVE queries when there is a potential problem with a document have a higher percentage of queries that do not verify on the initial attempt.

[16]Lawful status documents include, for example, a Permanent Resident Card.

[17]States are charged $0.50 for an initial or second SAVE verification request, and up to $2 for third requests.

Figure1: SAVE Initial Verification Rates, Fiscal Year 2011



Source: DHS data.
Note: Does not include data on queries submitted by the agency that issues non-driver identification cards in Hawaii.

Document Inspection

Another fraud prevention technique is inspection of identity documents by front-counter staff. In all the states we contacted, front-counter staff in local licensing offices inspects identity documents in an effort to detect counterfeits. This step is often done even for documents that are also verified electronically, such as SSN documents. Inspection generally involves the visual or physical examination of documents. Staff told us they look for security features embedded in authentic documents, such as watermarks and proper coloring in Social Security cards or raised seals on birth certificates. They may check if documents are printed on security paper that is used for authentic documents, and also to see if a document appears to have been tampered with. Staff may use a variety of tools to assist with their inspection. For example, they may use black lights and magnifying glasses. For certain types of documents, such as out-of-state drivers' licenses, they may consult books showing the most current versions of these documents. Staff in about half of the states we interviewed also used document authentication machines designed to detect counterfeit documents such as out-of-state licenses and passports. Officials in one of these states explained that front-counter staff scans certain types of documents into the machines, and the machines indicate if the document is authentic. Finally, training also plays a role in helping

staff inspect documents. Officials in all the licensing agencies we contacted said they have provided fraudulent document recognition training to their staff, which is also required by the REAL ID Act; most said that 100 percent of their staff have received such training. Even officials in states we contacted that have laws prohibiting implementation of the REAL ID Act said they have taken this step.

Facial Recognition and Other Biometric Techniques

Many states are using facial recognition techniques or fingerprinting which, while not required by the REAL ID Act, may detect applicants who attempt to obtain a license under an identity other than their own. According to AAMVA, licensing agencies in 41 states plus the District of Columbia were using facial recognition, fingerprinting, or both techniques as of June 2012.[18] Among the 11 states in our review, 5 routinely used biometric techniques as part of their verification procedures (4 used facial recognition and 1 used fingerprinting) and an additional 4 had plans to implement facial recognition procedures. Licensing agency officials in the remaining 2 states said they are barred by state law from using facial recognition to screen license applicants.

Facial recognition software analyzes an individual's photo and measures various aspects of the face, which may include the distance between different features such as the eyes, nose, and mouth. The unique set of measurements representing one facial image is compared to the measurements representing others, to detect images that are potentially associated with the same person. The states we interviewed that use facial recognition check each new license applicant's photo against all other photos of current license holders in their own state.[19] This check may detect applicants who try to obtain multiple licenses in the same state under different identities. These states may also compare the photo of an individual renewing a license to the photo on file for that license, to verify that both photos are of the same person. In the states we interviewed, facial recognition checks are typically run after the applicant leaves the local branch office but before a permanent license is mailed to

[18]AAMVA reported that licensing agencies in 40 states plus the District of Columbia were using facial recognition, 9 states were using fingerprinting, and 8 of these 9 were also among those using facial recognition.

[19]State licensing agencies generally perform facial recognition checks only against their own photo databases, according to the National Institute of Standards and Technology (NIST) which conducts studies on facial recognition.

an applicant.[20] These checks are not necessarily a purely automated function, and staff may need time to review images that are potential matches to determine if they really are of the same individual.

Additional Fraud Prevention Techniques

While states' facial recognition programs are focused on detecting in-state license fraud, states also have some procedures in place that may detect cross-state fraud. As of March 2012, 23 states and the District of Columbia were participating in a photo-sharing program facilitated by AAMVA that is designed to help detect fraud across state lines. This program allows a participating state to obtain the facial image associated with a surrendered license from the issuing state if that state also participates in the program. Through this process, a fraudulent license could be detected if a state query yields either no photo or a photo that does not match the applicant. In addition, state licensing agencies may detect cross-state fraud through other systems. For example, all states plus the District of Columbia participate in the Problem Driver Pointer System (PDPS), to check if license applicants have adverse driving records.[21] But by uncovering driving violations or other adverse licensing actions in other states, PDPS may also help states identify applicants who already have licenses in other states that they have not divulged. Also, a few state licensing agencies said they may use the National Law Enforcement Telecommunications System to check if a license applicant already has a license in another state. This system is generally only available to law enforcement personnel, not to all front-line staff in license issuance offices. Officials in one state told us they use it only in limited circumstances, such as when there is reason to suspect license fraud.

In addition to the variety of procedures states have in place to prevent fraud by license applicants, all the licensing agencies we interviewed have some internal control procedures that are intended to prevent fraud by their employees and ensure required procedures are followed. For

[20]Almost all of the states we interviewed issue some or all of their licenses or identification cards by mail from a central location. These states may provide applicants with temporary licenses at the front counter.

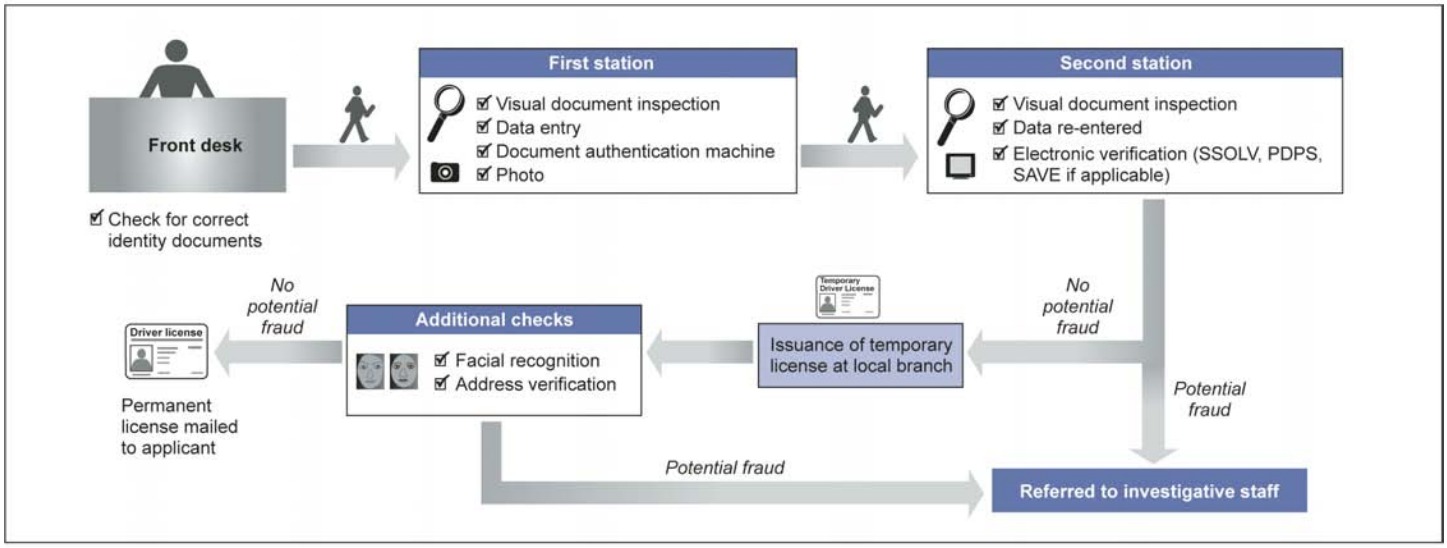
[21]The PDPS searches the National Driver Register, a database of state-provided driver information maintained by the Department of Transportation's National Highway Traffic Safety Administration, and if an individual is identified as having an adverse record, the PDPS "points" to the state where the individual's record may be obtained. A PDPS check is typically used to detect certain serious traffic violations or license suspensions or revocations associated with an applicant in other states, which might make the applicant ineligible to receive a license in a new state.

example, officials in almost all the states we interviewed said front-line staff may not override a non-match in an electronic verification system such as SSOLV in order to issue a license. Additionally, officials in most states told us managers examine licensing transactions to ensure proper procedures were followed. For example, officials in one state told us an audit team checks to make sure all required identity documents were collected as part of the transaction. Other procedures that states employ include monitoring licensing transactions to identify anomalies that may indicate internal fraud, such as the issuance of multiple duplicate licenses to the same individual; rotating staff among different stations so they do not know where they will be working on any particular day; and randomly assigning license applicants to the employee who will serve them, to avoid collusion.

Identity Verification: One State's Process

Figure 2 illustrates how the various systems and efforts work together to detect and prevent driver's license fraud in one of the states we reviewed. This state's process includes a number of the different types of checks we have described. An individual applying for a driver's license proceeds through two different stations, where several checks and other steps are performed by different employees. Certain steps are performed at one station only, such as taking the applicant's photo, checking documents with the authentication machine and performing the electronic verifications such as SSOLV. But other steps are performed at both stations, including entering data from identity documents into the licensing agency's computer system. State officials told us that having two employees enter applicants' data helps guard against internal corruption, because if one employee tries to collude with an applicant to enter false information, this will be caught by the other employee. If no potential fraud is found through all the checks at the local branch, the applicant is issued a paper license valid for 45 days. The licensing agency performs some additional checks after the issuance of the temporary license, including a facial recognition check against all photos in its database and verification that the applicant's mailing address is valid. If no concerns are found, the state mails a permanent license to the applicant.

Figure 2: Identity Verification Process in One State



Source: Interviews with state officials.

Although states are already implementing a number of the identity verification procedures required by the REAL ID Act, some states may not comply with certain provisions for various reasons. For example, officials in one state we interviewed said they are not verifying applicants' lawful status through SAVE because the state does not require people to have lawful status in the United States to obtain a license. Officials said the state has no plans to enact such a requirement. In other cases, state officials told us they find certain statutory or regulatory requirements to be burdensome or unnecessary. For example, several of the states we interviewed do not verify SSNs through SSOLV when individuals renew their licenses, a step required by DHS' regulations.[22] State officials told us it is not necessary to take this step because these SSNs were already verified at the time of initial license application; officials in one state also mentioned the cost of a SSOLV query as a reason not to re-verify an SSN.[23] DHS said one reason it is necessary to re-verify personal data such as SSNs for renewals is that such checks can detect cases where

[22]6 C.F.R. § 37.25.

[23]States must pay $0.05 for each SSOLV query.

the data are actually associated with a deceased individual.[24] Re-verifying SSNs may therefore detect attempts to renew a license fraudulently under the identity of a deceased individual. In addition, several of the states we interviewed do not require applicants to provide a document showing their SSN.[25] Officials in one of these states said the Social Security card is easy to tamper with so it is more valuable to verify the actual SSN than to assess the validity of the paper document. Officials in two states said they do not plan to comply with the deadlines in DHS' regulations, which will require states, after DHS has determined they are REAL ID-compliant, to process new applications and issue new licenses to certain license holders by 2014 and all license holders by 2017. These officials cited the expected resource burden of processing so many applications in a short period of time.

States Report Success in Preventing License Fraud but Cross-State Fraud and Counterfeit Birth Certificates Remain Challenges

States Report Success in Detecting Counterfeit Documents and Identity Theft

Officials in most of the states we interviewed said their anti-fraud efforts have had success in preventing the use of counterfeit documents to obtain licenses, especially documents associated with completely fictitious identities. Indeed, officials in the majority of our 11 selected states said they have seen a decline in attempts to obtain licenses using counterfeit documents. SSOLV makes it harder for criminals to obtain a license under a fictitious identity. Officials in most of the states we interviewed said SSOLV checks have helped make the use of fraudulent documents more difficult. For example, officials in one state told us that before it started using SSOLV, about 75 percent of license fraud cases

[24]See DHS's proposed rule, 72 Fed. Reg. 10,820, 10,838 (Mar. 9. 2007).

[25]DHS regulations require applicants to present a document that shows their SSN and specify which documents are acceptable. 6 C.F.R. § 37.11(e).

involved counterfeit Social Security cards, but the use of counterfeit documents such as these has declined significantly and is no longer the main type of fraud they see. Officials in several states also cited SAVE as having made the use of counterfeit documents more difficult. For example, officials in one state commented that when they started using SAVE in 2002 they identified many forged documents intended to prove lawful status in the United States, but over time they have seen fewer forgeries of these documents. Officials in several states said their efforts to train staff on fraudulent document recognition or to prevent corruption among their staff have also had an impact. Officials in one state said the use of counterfeit Social Security cards has declined partly because front-line staff is better trained on how to check documents for security features. Officials in another state told us internal control procedures, including having two staff separately inspect each document, has made license fraud more difficult to accomplish. Several states provided data indicating a decline in recent years in the number of license fraud investigations involving fraudulent documents. For example, one provided data showing a steady decline in the annual number of investigations based on referrals from front-counter staff, from 156 in 2002 to 36 in 2011. Officials said this trend reflects a decline in the use of counterfeit documents, because such cases are the ones typically detected by front-counter staff.

State officials also reported successes in using facial recognition technology to detect license fraud, particularly fraud involving identity theft. SSOLV has made it harder to get a license under a fictitious identity, but it cannot determine whether a valid SSN and other personal information (name and date of birth) submitted by a license applicant are truly associated with that applicant. Some evidence suggests that criminals seeking a license are now more likely to try to obtain one under another real identity—using genuine and sometimes forged identity documents to do so. For example, law enforcement officials in one state said that as the number of fraud cases involving counterfeit documents has declined, they have seen an increasing number of what they called imposter fraud: attempts to steal another person's complete identity—including name, SSN, and date of birth—and obtain a license under that identity. Officials in several states told us facial recognition plays an important role in preventing such fraud. Officials in one state, for example, said it is their most effective tool for detecting identity theft, and has detected over 100 license fraud cases annually since 2008. Officials in another state told us facial recognition has resulted in about 6,200 investigations and 1,700 arrests since its implementation in 2010. Officials in a few states told us after they introduced facial recognition

they detected individuals with a number of licenses under different identities—as many as 10 different identities associated with one individual in one case. However, state officials also said there are some limitations in the ability of facial recognition to detect matches between photos when a person's appearance has been altered in one photo. For that reason, among others, an official with NIST said facial recognition may be less effective than other biometric techniques such as fingerprinting and iris recognition in detecting matches.

Examples of How Facial Recognition Detected License Fraud

In one state we visited, licensing agency employees were issuing licenses to individuals using real identities of other people for payments of $7,500 to $12,500 a piece. As part of the scheme, these employees provided their customers with legitimate identity documents belonging to other people, such as Social Security cards and birth certificates. Facial recognition successfully identified that the individuals who had paid for the fraudulent licenses had already received other identification documents from the state and therefore had photos in the state's database. In another example from the same state, according to state officials, a foreign national who these officials identified as being on the "no-fly" list had obtained licenses under four different identities. This individual had been deported from the United States multiple times, and each time was able to re-enter the country under a different identity. Using facial recognition software, the state was able to detect him by comparing the photos associated with the different licenses.

License Fraud across State Lines and the Use of Counterfeit Birth Certificates Remain Challenges

States Remain Vulnerable to Cross-State License Fraud

States' vulnerability to license fraud perpetrated by individuals who cross state lines has been a longstanding issue, and it remains a challenge for states despite the success officials report in detecting other kinds of fraud.[26] Officials in the majority of states we interviewed told us their states bar their license holders from also holding licenses in other states, and the REAL ID Act also prohibits states from issuing a license to an applicant who already has one in another state. However, individuals may try to obtain licenses in multiple states. For example, criminals may try to

[26]We reported in 2003 that states were vulnerable to cross-state fraud because they lacked a means of systematically exchanging information about licensed drivers. See GAO-03-920.

get licenses under different identities by using the identity of someone who resides—and may have a license—in one state to obtain a license under that identity in a different state, perhaps to commit financial fraud under their stolen identity. Officials in all the states we interviewed acknowledged they lack the ability to consistently determine if the identity presented by a license applicant is already associated with a license-holder in another state. Some existing verification systems may accomplish this goal in limited circumstances but do not fully address the gap. For example, officials in a number of states told us a check against the problem driver database (Problem Driver Pointer System) will not detect a license in another state if it is not associated with any driving violation. Moreover, the national law enforcement data exchange system (National Law Enforcement Telecommunications System) is cumbersome to use if a state does not know which state an applicant may already have a license in, and in any case is generally only available to law enforcement personnel. Similarly, the AAMVA photo sharing program cannot be used to detect fraud if an applicant does not present an out-of-state license to be verified, and not all states participate. Finally, facial recognition programs generally only check a state's own internal photo database. They cannot detect cases when a criminal tries to obtain a license under the identity of someone else if neither of them have a license in the state.

Example of Cross-State Fraud

In one state an individual obtained an identification card under the identity of a person residing in another state by successfully using identity documents belonging to that person. The identity thief used this identification card as authorization to work. The crime was only discovered when the victim filed an identity theft complaint with the state in which the criminal obtained the fraudulent identification card and had been working.

States are trying to develop additional mechanisms for addressing cross-state license fraud, but none are fully operational yet. For example, a consortium of five states is developing a state-to-state verification system that would enable states to check if a license applicant's identity—including name, date of birth, and a portion of the SSN—is already associated with a license in other states. Officials in almost all the states we interviewed said such a system would be useful. Officials in several states said it could detect criminals who try to use the identity of someone in one state to obtain a license in another state—provided the identity theft victim is a license holder in the first state. However, officials in a number of states said there would be challenges to implementing such a system, primarily related to cost and ensuring the security of personal

data. The state consortium expects to complete its design work by 2013 and implement a pilot by 2015, but said it may not be until 2023 that the states have entered data on all their license holders into the system. Beyond the planned state-to-state system, some states have considered other approaches to addressing cross-state license fraud. Officials in several states told us cross-state facial recognition, in which states run checks against neighboring states' photo databases, could be a helpful tool. However, they cited obstacles, including the much larger number of potential matches that staff would have to examine, the technological incompatibility of different states' facial recognition programs, and privacy concerns. In addition, officials in one state suggested that it would be helpful if SSA informed states when an SSN submitted to SSOLV for verification had already been submitted previously, because this would alert states that someone might be fraudulently applying for licenses in multiple states. SSA officials said developing this capacity could slow down SSOLV response times and raise privacy concerns because SSA would need to store SSNs submitted by states. While AAMVA's photo sharing program can play a role in detecting certain kinds of cross-state fraud, the program's usefulness is limited because fewer than half the states currently participate, and AAMVA told us it lacks the resources to promote use of this program among additional states.

States Have Problems Identifying Forged or Fraudulently Obtained Birth Certificates

Even with the progress reported in preventing the use of certain types of counterfeit documents, the use of forged or improperly obtained birth certificates remains a challenge that leaves states vulnerable to license fraud. Officials in about half the states we interviewed said it can be challenging to detect counterfeit birth certificates. Officials in several states told us the wide variety of formats in which birth certificates are issued across the country makes detecting counterfeits difficult. According to NAPHSIS, there are thousands of different versions of birth certificates because formats vary over time and among issuing

agencies.[27] An official in one local license issuance office said his office often sees birth certificates from another state, where security features on birth certificates vary from county to county, and it can be difficult to keep track of all the variations. Besides forging birth certificates, criminals may improperly obtain someone else's genuine birth certificate. For example, criminals may steal or purchase the documents and use them as part of packages of identity documents to obtain licenses fraudulently. In other cases criminals may be able to obtain another person's birth certificate directly from a vital records agency. According to NAPHSIS, 15 states have virtually no restrictions on who may obtain a birth certificate from a vital records agency. Even in states that restrict access, there may be limited safeguards to ensure birth certificates are only provided to those who have a legitimate right to them. For example, officials at one vital record agency acknowledged that local staff who issue birth certificates do not receive fraudulent document recognition training, and a criminal with a sophisticated fake identification document such as a driver's license could use it to obtain someone else's birth certificate.

Example of Using A Forged Birth Certificate to Obtain a License Fraudulently

In one state an individual obtained a victim's personal data and applied for a license using a counterfeit birth certificate and counterfeit SSN documentation. This fraud was only discovered when the alleged criminal fled an accident involving a plane carrying narcotics, and checked into a nearby motel under the false identity.

A system exists that could help address the issue of counterfeit birth certificates and meet the REAL ID requirement to verify birth certificates with the issuing agency when they are submitted by license applicants, but state officials said there are challenges with using it and no states are currently doing so for this purpose. The Electronic Verification of Vital Events (EVVE) system is designed to verify the accuracy of data on birth

[27]The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the Department of Health and Human Services (HHS) to issue regulations setting certain minimum standards for birth certificates for acceptance by federal agencies, and to provide grants to assist states in conforming to the minimum standards and computerizing birth and death records, among other things. These minimum standards must include certain requirements specified in IRTPA, such as requiring the use of features designed to prevent tampering or counterfeiting, requiring proof and verification of identity as a condition of issuance, and establishing application processing standards to prevent fraud. Pub. L. No. 108-458, § 7211, 118 Stat. 3638, 3825-27 (2004), codified at 5 U.S.C. § 301 note. According to HHS's Semiannual Regulatory Agenda published in February 2012, the agency estimated publishing a Notice of Proposed Rulemaking in September 2012; however, as of September 11, 2012, HHS had not yet done so. 77 Fed. Reg. 7945, 7948 (Feb. 13, 2012).

certificates including name, date of birth, and either the date the certificate was filed or the file number.[28] It is operated by NAPHSIS, the organization that represents the nation's vital records agencies. As of February 2012, 43 of 57 vital records agencies were participating in the system, meaning at least some of their birth records could be electronically verified.[29] Licensing agencies in three states participated in a multi-year pilot ending in 2011, in which they used the system to verify birth certificates for license applicants. Officials in one of the pilot states told us that, based on their experience, EVVE has the potential to help detect counterfeit birth certificates, because while criminals may be able to obtain another person's name and date of birth and create a counterfeit birth certificate, it is more difficult to obtain the correct file date on the victim's birth certificate—which must match to pass an EVVE check. However, officials in this state cited challenges they experienced during the pilot, including confusion about which date on the birth certificate is the file date that should be entered for verification and gaps in the state's vital records data which make verification difficult for birth certificates filed during certain periods of time. Similarly, officials in most of the states we interviewed that had not participated in the pilot said it could be helpful to use EVVE, but also expressed concerns about the cost of using the system, the fact that not all vital records agencies are participating, and the completeness or accuracy of the vital records data that are already available for verification through it. As an interim solution, some licensing agencies are working towards verifying at least their own states' birth records electronically. Officials in several of the licensing agencies we interviewed have considered or are planning to start working with the vital records agencies in their states to electronically verify birth records for license applicants born in-state. Officials in one licensing agency told us they have discussed this approach with the vital records agency in their state, and see it as an interim step before EVVE is more viable. Licensing

[28]Several other federal and state agencies use EVVE, including SSA and Medicaid offices in some states.

[29]The 57 vital records jurisdictions that issue birth certificates are the 50 states, the District of Columbia, New York City, American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands. The vital records agencies in these jurisdictions vary widely in the extent to which they maintain birth records in electronic databases, which is necessary for these records to be available for verification through EVVE. For example, as of February 2012 one agency had electronic records for births back to 2004, while some others had electronic records back to around 1900. But even some vital records agencies with extensive electronic records were not participating in EVVE as of February 2012.

agencies face obstacles in these efforts, though, such as birth records not being fully in electronic format or the reluctance on the part of vital records agencies to participate in electronic birth record verification arrangements.

GAO Investigative Work Highlights Vulnerabilities

Our investigative staff exploited the vulnerabilities discussed above to fraudulently obtain drivers' licenses in the three states where we made such attempts. In each state, investigative staff obtained genuine licenses under fictitious identities—combinations of name, date of birth, and SSN that do not correspond to any real individuals. In two states, a staff member obtained two licenses under two different identities. In each attempt, staff visited local license issuance branches and submitted various counterfeit documents to establish their identities, depending on state requirements. In all cases they submitted a counterfeit driver's license and a counterfeit birth certificate, both purportedly from other states. (See figure 3 below for examples of the counterfeit birth certificates used.) In some cases, staff also submitted other documents including fake Social Security cards and fake pay stubs. In most of these five attempts across the three states, we were issued permanent or temporary licenses in about 1 hour or less. In only one case did a front-counter clerk appear to question the validity of one of the counterfeit documents, but this clerk did not stop the issuance process. All three states check the validity of applicants' personal data—including SSN—through SSOLV, but assuming SSOLV checks were performed, they were not sufficient to detect these fraud attempts because the SSNs were valid.[30]

[30]We used SSNs that are valid, in the sense that they exist in SSA's database, but that do not correspond to any real individual.

Figure 3: Counterfeit Birth Certificates Used by GAO Investigative Staff

CERTIFIED TRANSCRIPT OF BIRTH
STATE OF NEW YORK
DEPARTMENT OF HEALTH

FULL NAME OF CHILD: [redacted]
DATE OF BIRTH: April 30, 1956
PLACE OF BIRTH: White Plains, New York
MAIDEN NAME OF MOTHER: [redacted]
NAME OF FATHER: [redacted]
DATE FILED: July 17, 1956
STATE FILE NO.: 01469

This is to certify that the information concerning the birth of the above named person is a true and accurate transcription of the information recorded on the original certificate of birth on file with the New York State Department of Health.

Peter M. Carucci
Director, Vital Records Section
DATE August 16, 2002

CERTIFIED COPY

Do not accept this transcript unless the certified copy Certificate of Live Birth raised seal is affixed thereon.

ANY ALTERATION VOIDS THIS TRANSCRIPT

DOH 4055 (4/2001) X448111219-1 -V4228

United States of America

State of West Virginia, County of Ohio, ss:

Birth Certificate

I, Chester W. Kloss, Clerk of the County Commission, in the County and State aforesaid, it being an office of records, and having a seal, do hereby certify that the records in my office show that:

[redacted] was born in Wheeling County of Ohio and State of West Virginia on the 14th day of February 1947
Sex Male Race White and the parents names are as follows:
Father's Name [redacted] Age of Father 40
Mother's Maiden Name [redacted] Age of Mother 31
as shown by certificate of birth returned by Joseph N. Perdue, MD, and recorded in Birth Record No. 1949-0124 at page 3 Certificate filed July 17, 1949

CERTIFIED COPY

In testimony whereof, I have hereunto affixed my signature and official seal at Wheeling, West Virginia, this 7th day of December 1991

Clerk of Ohio County Commission Wheeling, WV 26003

Source: GAO.
Note: These birth certificates contain fictitious information, which does not correspond to any real individuals.

These successful fraud attempts demonstrate several vulnerabilities in states' defenses against license fraud. First, the fact that we were able to use counterfeit out-of-state licenses in each attempt further confirms states' inability to consistently check if applicants' identities are already associated with licenses in other states. If the envisioned state-to-state verification system were in place, then the states where we applied might have discovered that the out-of-state licenses we submitted were fakes and did not actually exist. Under current plans, this system would verify the validity of licenses submitted from other states as well as check if applicants have licenses from other states that they have not divulged. Even in the absence of the state-to-state system, if all states participated in AAMVA's photo sharing program, then the counterfeit out-of-state licenses might have been detected through a request to the purported

state of origin of the license to validate it. We specifically selected states for our undercover work that are not among the 23 participating in this program. But as long as any states are not participating, criminals could present counterfeit licenses from these states, and even participating states would be vulnerable. The second vulnerability relates to birth certificates. We were likely able to use counterfeit birth certificates containing fictitious information because no state licensing agencies are verifying birth certificate data through EVVE. None of the front-line clerks in the offices where we applied for licenses questioned the validity of the counterfeit birth certificates presented. Finally, the third vulnerability is that some states are still not using facial recognition or other biometric techniques to detect identity theft. The fact that the two states where our staff applied for multiple licenses are among the nine states that do not use facial recognition technology or other biometric techniques most likely made it easier in these states for our staff to obtain two licenses under two different identities. Facial recognition checks may be able to detect multiple licenses associated with the same individual. While it might still be possible for a criminal to obtain a license fraudulently even if all states utilized a state-to-state verification system, EVVE, and facial recognition, use of these systems would likely have increased the chances of detecting our fraudulent license applications.

SSA and DHS Have Enhanced Verification Systems but DHS Has Not Provided Adequate Guidance on REAL ID Implementation

Agencies Have Improved Existing Systems and Helped States Develop New Verification Systems

SSA has taken actions that enhance licensing agencies' ability to verify SSNs and other personal data. Specifically, the agency has addressed two areas of concern that we raised in 2003.[31] First, to enhance the level of service provided to states, SSA established performance goals, including hours when SSOLV is to be available and response times. Second, to address a vulnerability that might leave states open to license fraud by criminals stealing the identity of a deceased individual, SSA now automatically checks all inquiries against its death records.

DHS has similarly taken several actions to improve the usefulness of SAVE. To improve data accuracy and verification rates, the agency monitors verification rates in order to identify problems with data accuracy in the databases SAVE accesses, which contribute to unsuccessful initial verification attempts. Officials in several of the states we interviewed acknowledged that DHS has been taking steps to improve verification rates, the timeliness of query responses, and the accuracy of underlying data, and these officials reported improvements in these areas. In addition, DHS has recently developed a new portal for accessing and using SAVE. Known as the Verification of Lawful Status (VLS) system, it will be accessible through AAMVA's electronic hub for accessing other verification systems such as SSOLV. DHS is pilot testing VLS, with roll out to all states planned by the end of fiscal year 2012. Officials in several states told us they believe this new approach will make it easier for them to use SAVE more consistently or extensively. Officials in two states, in

[31]We reported that SSOLV was often overwhelmed by the number of verification requests, that it experienced frequent outages, and that SSA had not sufficiently focused on management of the system. In addition, SSA did not check whether SSNs submitted through the batch method were associated with deceased individuals. See GAO-03-920.

fact, said the deployment of VLS would enable them to start using the system in the future. DHS has conducted webinars for licensing agency staff on using SAVE, and it is developing online training modules that DHS officials say will also include instruction on interpreting verification results.

Beyond these efforts to improve existing verification systems, DHS has provided financial assistance to support states' efforts to develop new verification systems that could be used to comply with the REAL ID Act. Section 204 of the REAL ID Act authorizes grants to assist states in conforming to the minimum standards in the Act. DHS has awarded about $63 million through various grants since 2008 for upgrading the communications and verification systems infrastructure including development of the state-to-state system and pilot testing other systems. All of these funds were awarded to a group of five states that were part of a consortium that was formed for this purpose. At least half of the $63 million is being used by the consortium for the development and implementation of the state-to-state system, and these funds are available through fiscal year 2016. DHS officials said these funds are designed in part to induce states to start using the system, but in the longer term, the agency expects states to pay for the operation of the system. Besides funding support, DHS has also provided technical advice to help the states understand the federal requirements the system must meet. In addition to the funds set aside for the state-to-state system, some of the grants were also used to support a pilot project in which licensing agencies verified birth certificates through EVVE.[32] However, based on a recommendation from the consortium, DHS does not plan to provide any additional financial support to state licensing agencies for further pilot testing of EVVE because of high transaction costs charged by state vital records agencies. DHS officials are also concerned about inaccuracies in electronic birth records that may lead to non-verifications, and the fact that EVVE checks may still be evaded by people who obtain someone else's birth certificate in one of the states where birth records are accessible to the general public.[33]

[32]Besides the state-to-state system and EVVE, the state consortium has also been involved in piloting some other systems.

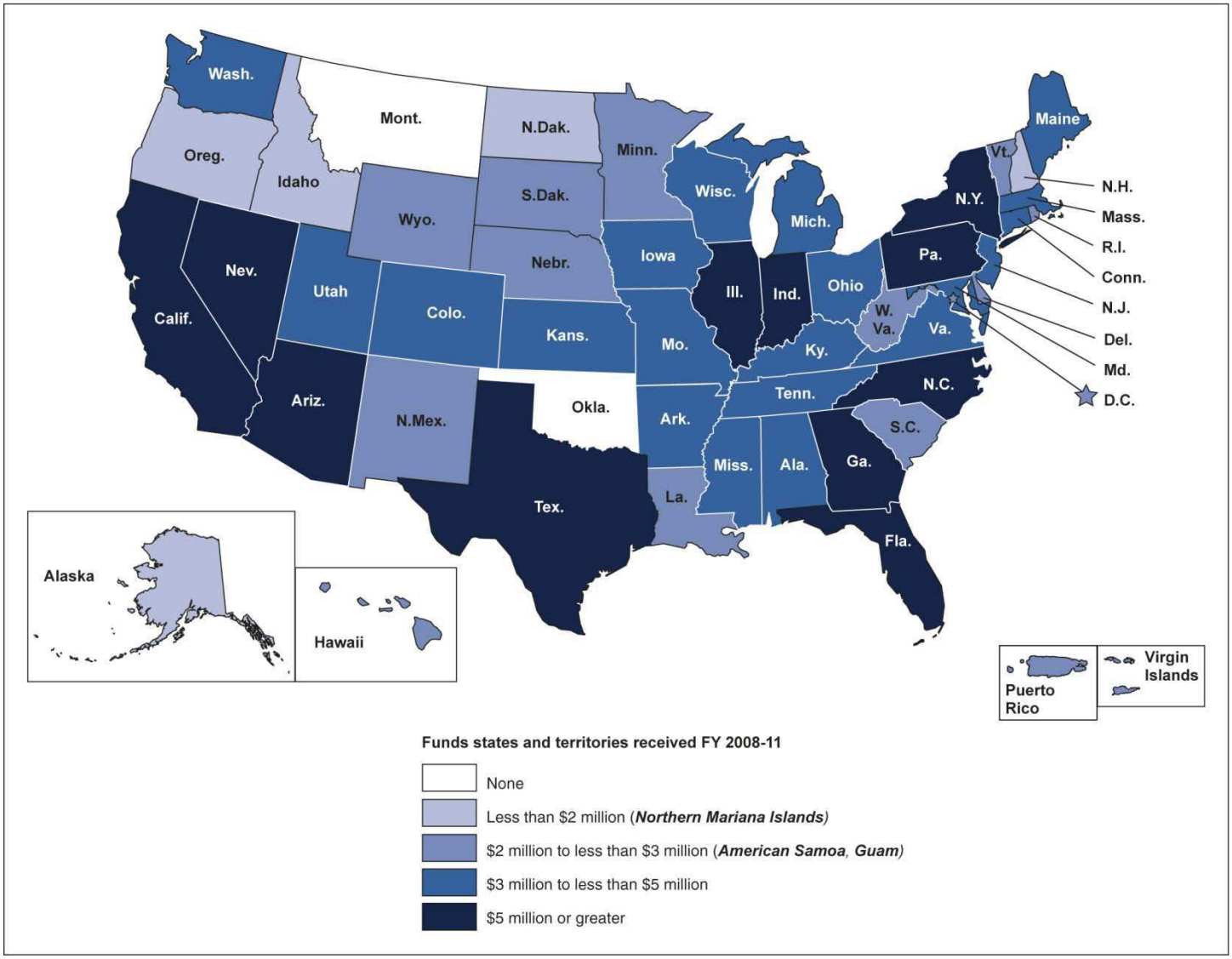
[33] As a means of addressing this problem, DHS officials told us the agency is exploring testing a system in which state vital records offices would verify the driver's license or identification cards of persons who request copies of their birth certificate.

DHS has also provided grants to individual states to help them improve their driver's license security procedures, including identity verification. The Driver's License Security Grant Program (DLSGP) provided over $200 million in grants to states and territories from fiscal years 2008 to 2011.[34] All but 2 states applied for and received grant funds during this time period (see fig. 4).[35] Initially established as the REAL ID Demonstration Grant program, the DLSGP provides assistance to states for improving the security and integrity of their drivers' licenses in ways that are consistent with the requirements of the REAL ID Act. Both states with and without laws opposing implementation of the REAL ID Act were eligible to apply for and received these grants. Funds could be used for planning activities, equipment purchases, equipment maintenance and repair, and related costs. Officials in states we interviewed said they used their funds for efforts such as installing or updating facial recognition systems, providing staff anti-fraud training and information sharing, and in one case supporting efforts by the state's vital records agency to digitize its birth records.

[34]No DLSGP grants were awarded in fiscal year 2012 because the funding for those purposes was consolidated with that of several other programs into another program called the State Homeland Security Grant Program.

[35]Under the fiscal year 2011 allocation formula, each state or territory received a base amount with the balance based upon the number of licenses and identification cards issued.

Figure 4: REAL ID Demonstration Grant and Driver's License Security Grant Program (DLSGP) Funds Distributed to States and Territories, Fiscal Years 2008 – 2011



Source: GAO analysis of DHS data; Map Resources (map).

Note: Montana and Oklahoma did not apply for grants during this time.

DHS has conducted other activities that may help combat license fraud generally, and officials in several of the states we interviewed told us they were participating in these efforts. However, these efforts are broad in

nature and are not specifically designed to support compliance with the REAL ID Act. For example, DHS operates a forensic laboratory that investigates the use of counterfeit identity documents and is a resource available to driver licensing agencies. DHS also leads task forces involving federal, state, and local law enforcement agencies that are designed to combat identity document fraud, including driver's license fraud. These task forces seek to pursue criminal prosecutions and financial seizures.

DHS Has Not Provided Comprehensive Guidance to Help States Implement the REAL ID Act

Despite the approaching January 2013 deadline for compliance, DHS has not provided timely, comprehensive, or proactive guidance on how states seeking REAL ID compliance could meet the identity verification requirements. For example, DHS did not issue written guidance on how to meet specific REAL ID Act identity verification requirements for over 4 years after it issued its final regulations in 2008.[36] Officials in most of the states we interviewed expressed a need for additional guidance on how they could meet the identity verification requirements of the REAL ID Act and DHS regulations. Because of this lack of guidance, officials in these states said they are uncertain as to whether they will be in compliance with various provisions when the law goes into effect, and some are concerned about investing resources in particular steps only to find out afterwards that they are not in compliance. For example, officials in one state said there was a lack of clarity about whether military identification cards may be used to prove identity under the REAL ID Act. In the absence of formal written guidance, they have often had to make assumptions based in part on DHS officials' informal remarks.

The guidance DHS has provided regarding verification of license applicants' identities has generally been ad hoc or in response to state requests. For example, DHS provided additional information to states in June 2012 in the form of answers to frequently asked questions posted to its website.[37] Moreover, agency officials previously indicated that DHS was planning to issue a comprehensive guidance document specifying

[36]DHS issued guidance in 2009 on implementing REAL ID Act requirements other than those for license applicant identity verification. These include *REAL ID Mark Guidelines,* and the *REAL ID Security Plan Guidance Handbook* which primarily address license document security features and security requirements for licensing facilities respectively.

[37]See http://www.dhs.gov/files/programs/secure-drivers-licenses.shtm.

actions states could take to meet REAL ID Act requirements and what states should cover in the certification plans they submit to DHS for approval. However, DHS officials said they are now reevaluating that decision. Agency officials said DHS will continue to provide additional guidance as needed through the frequently asked questions web page, presentations at conferences of state licensing agency officials, or responses to specific questions from individual states. However, state officials reported mixed experiences with how DHS has responded to their specific questions. On the one hand, officials in several states said DHS has been responsive to questions they had on meeting particular REAL ID Act requirements. For example, officials in one state said DHS has for the most part responded relatively quickly to e-mail inquiries. On the other hand, however, officials in some states cited instances in which DHS has not responded promptly, or at all, to their questions. For example, officials in one state told us they had not received a response to a question they first asked DHS in 2009 about whether enhanced drivers' licenses would meet REAL ID Act requirements.[38] Officials in another state told us it took longer than they expected for DHS to respond to a question about whether refugees and asylum seekers should be treated as permanent U.S. residents when they apply for a license.

DHS guidance is especially critical for two key REAL ID Act requirements—not issuing licenses to persons who already have them from other states and verifying birth certificates—given that the electronic verification systems designed for those purposes will not be fully operational for years, and the approaching deadline for states to submit their compliance plans. DHS regulations require states to use electronic verification systems as they become available, but also authorize states to use alternative methods approved by DHS.[39] However, in addition to not providing comprehensive guidance specifying what alternative procedures would be acceptable for compliance with these requirements, DHS officials also indicated they have no plans to promote certain strategies they consider potentially useful that might partially help states meet these requirements, such as: (1) expansion of the AAMVA photo

[38]Enhanced drivers' licenses are augmented with additional security features and approved by DHS for use as proof of identity and U.S. citizenship in place of a passport for entry into the United States by land or sea from Canada, Mexico, Bermuda, and the Caribbean. In its June 2012 frequently asked questions, DHS stated that enhanced drivers' licenses are acceptable for official federal purposes.

[39]6 C.F.R. § 37.13(b).

sharing program to additional states, and (2) expansion of licensing agencies' efforts to verify birth certificates through their own states' birth records for applicants born in-state. Instead, DHS plans to consider alternatives states propose in their compliance plans. DHS officials said they believe this approach gives states opportunities to develop innovative solutions and flexibility to consider their own circumstances. However, officials in some states we interviewed expressed a need for direction from DHS to help identify possible alternatives. Officials in one state we interviewed, for example, wanted assistance in identifying what procedures could be followed to meet these requirements until the state-to-state verification system and EVVE are fully operational. Officials in another state told us that in their view, DHS would need to provide additional options for meeting these requirements in order for DHS to determine states are compliant by January 2013.

Conclusions

Since the terrorist attacks of September 11, 2001, states have largely closed off certain approaches that identity thieves and terrorists have used to fraudulently obtain drivers' licenses, and federal actions have contributed to this progress by enhancing verification systems or by providing financial support to help states develop new systems. But, as our investigative work demonstrates, it is still possible to exploit several remaining vulnerabilities in states' identity verification procedures to fraudulently obtain genuine drivers' licenses, contrary to the purpose of the REAL ID Act. DHS has provided some guidance about certain aspects of REAL ID implementation primarily in response to state questions. However, the lack of proactive guidance by DHS on interim solutions for certain REAL ID Act requirements has hampered states' ability to fully address these gaps. For example, even though the state-to-state system is still years from fruition, there are opportunities before the system's expected completion date of 2023 for states to at least partially address the REAL ID requirement to prevent people from getting multiple licenses from different states—and thereby close off certain paths to cross-state fraud. But without guidance and encouragement from DHS, states and other agencies may be less likely to coordinate in pursuit of these opportunities. Similarly, even though EVVE is not yet fully operational, states can still make it harder for criminals to use forged birth certificates by, for example, checking their own birth records for license applicants born in-state. However, without leadership from DHS, states and other agencies may be less likely to coordinate in pursuit of these opportunities or see the value in taking action. Additionally, in the absence of an effective DHS strategy to help states address these REAL ID Act requirements and high-risk vulnerabilities while the national

systems are being developed, states may elect not to comply with the Act, may invest in ad hoc or stopgap measures that are not sufficient for compliance, or most importantly, may be ill-equipped to adequately combat this type of fraud.

Recommendations for Executive Action

To enhance state driver licensing agencies' ability to combat driver's license fraud, consistent with the requirements of the REAL ID Act, we recommend that the Secretary of Homeland Security take the following interim actions while national systems to detect cross-state and birth certificate fraud are being developed:

1. Work with state, federal and other partners to develop and implement an interim strategy for addressing cross-state license fraud. Such a strategy could include, for example, expansion of AAMVA's photo sharing program or enhanced utilization of SSOLV to identify SSNs that are queried multiple times by different states. This strategy should include plans for sharing best practices and ideas for alternative solutions among the states.
2. Work with states and other partners to develop and implement an interim strategy for addressing birth certificate fraud. Such a strategy could include, for example, coordination between driver licensing agencies and state vital records agencies to verify birth certificates for license applicants born in-state.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and SSA for review and comment. In its written comments (see app. I), DHS did not concur with either of our recommendations, saying that interim strategies for addressing cross-state and birth certificate fraud are not needed. The agency said it has informed states that existing systems and procedures may address these issues and meet regulatory requirements, and has provided grant funds to help states develop their own new solutions. DHS emphasized that states need the flexibility to adopt solutions that best fit their individual circumstances. We acknowledge in our report that DHS has supported states' efforts to address cross-state and birth certificate fraud in the ways it outlines in its comments. However, we continue to believe that DHS needs to assume a more proactive role in these areas—and that it is possible to do so without being overly prescriptive. State driver licensing agencies remain vulnerable to cross-state and birth certificate fraud. Existing systems and methods are not sufficient to address the vulnerabilities, as our undercover work demonstrates. Given the anticipated date (2023) for full implementation of the state-to-state

system, and the continuing issues with driver licensing agencies' use of the EVVE system, states need new interim solutions and alternatives now. And, officials in many of the states we contacted still said they are confused about how to comply with certain REAL ID provisions, such as those related to cross-state and birth certificate fraud, despite DHS' efforts to provide information through conferences and responses to individual state questions. A formal strategy for addressing these vulnerabilities in the short term that is made available to all states in a consistent manner would better enable states to learn about and implement new options. Furthermore while DHS notes in its comments that HHS has a statutory responsibility for setting minimum standards for birth certificates, DHS involvement in this area is also critical because establishing date of birth is a central part of the driver's license application process. DHS also provided technical comments, which we incorporated as appropriate.

In its written comments (see app. II), SSA asked that we remove from our first recommendation the reference to enhanced utilization of SSOLV as one option for detecting cross-state fraud. As SSA notes, we do acknowledge in our report that there may be challenges with such use of SSOLV. Accordingly, our recommendation does not direct DHS and SSA to proceed with modifying SSOLV. It directs DHS to consider, in consultation with relevant partners, the enhanced use of SSOLV as one of a range of options for addressing cross-state fraud. We expect that DHS and SSA would more thoroughly evaluate the potential benefits and challenges of using SSOLV for this purpose and jointly determine whether to include this option in an overall strategy for combating cross-state fraud. Consequently, we made no change in response to this comment. SSA also provided technical comments which we incorporated as appropriate.

We are sending copies of this report to the relevant congressional committees, the Secretary of Homeland Security, the Commissioner of Social Security, and other interested parties. This report is also available at no charge on GAO's website at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact me at (202) 512-7215 or bertonid@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Staff members who made key contributions to this report are listed in appendix III.

Daniel Bertoni, Director
Education, Workforce, and Income Security Issues

Appendix I: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 10, 2012

Mr. Daniel Bertoni
Director, Education, Workforce, and Income Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-12-893: "DRIVER'S LICENSE SECURITY: Federal Leadership Needed to Address Remaining Vulnerabilities"

Dear Mr. Bertoni:

Thank you for the opportunity to comment on the draft report on the Department of Homeland Security's (DHS's) work with states in addressing driver's license security. We appreciate the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review.

DHS is pleased with GAO's recognition that several officials from the states surveyed acknowledged the Department in taking steps to improve the usefulness of the Systematic Alien Verification for Entitlements (SAVE) database through improved verification rates, timeliness of query responses, and accuracy of data. DHS also provided technical and financial assistance, including about $263 million in grants awarded since 2008.

The draft report contained two recommendations with which the Department non-concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Work with state, federal and other partners to develop and implement an interim strategy for addressing cross-state license fraud. Such a strategy could include, for example, expansion of AAMVA's photo sharing program, or enhanced utilization of SSOLV to identify SSNs that are queried multiple times by different states. This strategy should include plans for sharing best practices and ideas for alternative solutions among the states.

Response: Non-concur. DHS does not agree that an "interim strategy" is needed. We have worked and will continue to work with state, federal and other partners to identify alternate methods for addressing cross-state license fraud and ensure those ideas and best practices are shared.

DHS supports states having the flexibility to adopt innovative solutions and leverage emerging technologies to implement strategies best suited to their individual needs. For example, DHS has

worked extensively with the Social Security Administration (SSA) to fund and implement improved capabilities for Social Security Online Verification (SSOLV).

Also, DHS has suggested, in multiple venues, that the use of existing state-to-state systems such as the Commercial Driver's License Information System (CDLIS) and Problem Driver Pointer System (PDPS) and requiring applicants to surrender licensees issued by other states would satisfy regulatory requirements. States are encouraged to use a combination of these systems to ensure the validity of source documents by identifying and/or implementing controls to combat fraud and identity theft.

In addition, DHS has made funding available to states and listed such projects as eligible uses of grant funds. States have been given latitude in how they use these funds. In some cases, states may have significant restrictions on the sharing of biometric data.

Finally, DHS provided more than $63 million to the Driver's License/Identification Verification Systems (DIVS) consortium of 27 states led by the state of Mississippi to review, prioritize, and recommend solutions to the issues raised in this report. To the extent possible, DHS approved and funded the solutions and projects recommended by the states themselves. While some states have chosen not to participate in the DIVS consortium and individual states may not endorse all aspects of each and every project, the strategies and tactics have been designed and implemented by the states, not DHS.

Recommendation 2: Work with states and other partners to develop and implement an interim strategy for addressing birth certificate fraud. Such a strategy could include, for example, coordination between driver licensing agencies and state vital records agencies to verify birth certificates for license applicants born in-state.

Response: Non-concur. DHS does not agree that an "interim strategy" is needed. We continue to work with states and other partners to identify common methods and best practices for addressing birth certificate fraud and ensure those ideas and best practices are shared.

DHS supports states having the flexibility to adopt innovative solutions and leverage emerging technologies to implement strategies best suited to their individual needs. Common methods used to satisfy the birth certificate verification requirement include the thorough inspection of the document by an employee trained in recognizing fraudulent documents, the comparison of birth certificate information with other identity information presented, and the electronic verification of data (e.g., social security information) using available information technology (IT) systems.

Also, the Department of Health and Human Services (HHS) has the lead role in combating birth certificate-related fraud. The Intelligence Reform and Terrorist Prevention Act (IRTPA) of 2004 (§7211 of Pub. L. 108–458, 5 U.S.C. §301 note) assigns HHS with responsibility for setting minimum standards for birth certificates and for awarding grants to assist states in meeting the minimum standards, to computerize birth and death records, and foster the capability for electronic matching.

Additionally, under the leadership of the state of Mississippi, the DIVS consortium of states has funded, and is continuing to fund a variety of projects to address the birth certificate fraud issues identified in this report. The state of Mississippi has already funded: (1) system improvements to Electronic Verification of Vital Events (EVVE) and related systems; (2) pilot projects to test the new capabilities; and (3) detailed White Papers and empirical studies of the benefits and costs of state use of EVVE for verification of birth certificates.

Moreover, DHS has already awarded funding to the state of Mississippi to develop and test capabilities that will enable State Vital Records Agencies to electronically validate driver's licenses presented by customers seeking copies of birth certificates. From the beginning, DHS has consistently committed to supporting state recommended solutions to state problems in meeting the verification requirements of the REAL ID Act.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

for Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

3

Appendix II: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

September 05, 2012

Mr. Daniel Bertoni
Director
Education, Workforce and Income Security
U.S. Government Accountability Office
441 G. Street, NW
Washington, D.C. 20548

Dear Mr. Bertoni:

Thank you for the opportunity to review the draft report, "DRIVER'S LICENSE SECURITY: Federal Leadership Needed to Address Remaining Vulnerabilities" (GAO-12-893). Please see our enclosed response.

If you have any questions, please contact me at (410) 965-0520. Your staff may contact Amy Thompson, Senior Advisor for Records Management and Audit Liaison Staff, at (410) 966-0569.

Sincerely,

Dean S. Landis
Deputy Chief of Staff

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE DRAFT REPORT, "DRIVER'S LICENSE SECURITY: FEDERAL LEADERSHIP NEEDED TO ADDRESS REMAINING VULNERABILITIES" (GAO-12-893)

RECOMMENDATIONS

The Secretary of Homeland Security should take the following interim actions while national systems to detect cross-State and birth certificate fraud are being developed:

1. Work with State, Federal and other partners to develop and implement an interim strategy for addressing cross-State license fraud. Such a strategy could include, for example, expansion of AAMVA's photo sharing program, or enhanced utilization of SSOLV to identify SSNs that are queried multiple times by different States. This strategy should include plans for sharing best practices and ideas for alternative solutions among the states.

2. Work with States and other partners to develop and implement an interim strategy for addressing birth certificate fraud. Such a strategy could include, for example, coordination between driver licensing agencies and State vital records agencies to verify birth certificates for license applicants born in-State.

RESPONSE

In May 2012, GAO discussed with us the possibility of modifying the Social Security Online Verification (SSOLV) system to identify SSNs queried by multiple states. The discussion focused on the functional capabilities of the SSOLV system, but we also described existing legal and privacy constraints that prevent expanding the use and disclosure of SSOLV system data. We appreciate that GAO acknowledged some of our concerns on page 18 of the report, where it states that changes to the SSOLV system would "slow down SSOLV response times and raise privacy concerns." However, the report does not contain an evaluation of the legal, privacy, technical, and financial impediments associated with altering SSOLV in order to reduce cross-State driver license fraud.

We are legally required to verify names and Social Security numbers using the SSOLV system. Making the drivers' license issuance process more secure and enforcing transportation laws are within the purview of the Department of Homeland Security and the Department of Transportation, not SSA.

For these reasons, we ask you to delete the phrase, "or enhanced utilization of SSOLV," from the first recommendation.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Daniel Bertoni, 202-512-7215 or bertonid@gao.gov

Staff Acknowledgments

In addition to the contact named above, Lori Rectanus, Assistant Director; Lorin Obler; Joel Marus; Susannah Compton; John Cooney, Jr.; Sarah Cornetto; Keira Dembowski; Holly Dye; Robert Graves; Dana Hopings; Kristy Kennedy; Otis Martin; Mimi Nguyen; George Ogilvie; Almeta Spencer; and Walter Vance made key contributions to this report.

Related GAO Products

State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud. GAO-10-922T. Washington, D.C.: July 29, 2010.

Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain. GAO-09-759T. Washington, D.C.: June 17, 2009.

Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring. GAO-08-1009R. Washington, D.C.: September 19, 2008.

Social Security Numbers: Use Is Widespread and Protection Could Be Improved. GAO-07-1023T. Washington, D.C.: June 21, 2007.

Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain. GAO-07-752. Washington, D.C.: June 15, 2007.

Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. GAO-07-737. Washington, D.C.: June 4, 2007.

Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data. GAO-06-674. Washington, D.C.: June 26, 2006.

Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs. GAO-06-495. Washington, D.C.: May 17, 2006.

Social Security Numbers: More Could Be Done to Protect SSNs. GAO-06-586T. Washington, D.C.: March 30, 2006.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way. GAO-05-710. Washington, D.C.: June 30, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification. GAO-03-920. Washington, D.C.: September 15, 2003.