Center for Immigration Studies

Backgrounder

February 2012

REAL ID Implementation Annual Report

Major Progress Made in Securing Driver's License Issuance Against Identity Theft and Fraud

By Janice Kephart

Introduction

The September 11 hijackers had between them 30 state-issued driver's licenses and non-driver identification cards. These IDs were used not only to board airplanes but also to navigate in our society in preparation for the attacks. This is why the 9/11 Commission recommended a tightening of ID standards and why Congress in 2005 passed the REAL ID Act.

This report is an attempt to provide a comprehensive assessment of how well states are doing in improving driver's license issuance standards of the REAL ID Act. The Act was designed to protect identities and driver's license and identification cards while eliminating fraud and improving the customer experience. REAL ID contains 39 benchmarks; only the most important are covered here, grouped into eight categories, and presented in the table that forms the heart of this report (see pp. 10-12).

Overall the report finds that there is substantial compliance sought across the board by all states and territories (56 jurisdictions in all), even if there remains a wide gap between the strongest of state systems and the weakest. (References below to "states" may include the 50 states, the District of Columbia, or the five island territories.) This assessment found that almost every jurisdiction is continuing to improve its credentialing, even if some state statutes prevent actual REAL ID compliance. Even jurisdictions where there are too few improvements are not stagnant, but are working to improve aspects of issuance either with technology vendors or the American Association of Motor Vehicle Administrators (AAMVA), the entity that is responsible for promulgating many driver's license standards as well as providing much of the network support for information-sharing that state motor vehicle agencies use.

This assessment concludes that states (1) see tremendous value in pursuing REAL ID standards in reducing fraud, increasing efficiencies, improving customer service, and supporting law enforcement; (2) are willing to pay for those improvements with their own budgets outside of federal grant monies; and (3) are often exceeding REAL ID minimum standards in order to achieve more complete credentialing security. This study finds that:

- 53 states and territories are embracing REAL ID or the technical tenets of REAL ID.
- Five states have submitted REAL ID compliance packages to the Department of Homeland Security and 36 are materially or substantially materially compliant now or likely will be by the REAL ID compliance deadline of January 15, 2013.
- Of the 36, nine states are or will be issuing "gold star" licenses which are specially branded for acceptance for security screening at commercial airports and entering certain federal facilities. Another 27 have met or will meet the first 18 "material compliance" benchmarks that have been used for years as a measure of compliance. This includes the four states issuing enhanced driver's licenses that meet REAL ID material compliance tenets produced for the State Department for border crossing, with Minnesota to be the fifth to begin production.

Janice Kephart is the Director of National Security Policy at the Center for Immigration Studies. *Thank you to Andrew Meehan for research support.*

- Seven states have made improvements, but are not likely to meet material compliance.

- Among all 56 states and territories:

  - At least 43 are issuing tamper-resistant cards;

  - 51 are checking SSNs and the remaining five are currently getting online;

  - 47 are registered with DHS to check legal presence through the SAVE database, two are coming online, and seven are not (two have statutes preventing this check);

  - Nearly all vital record agencies have digitized their vital events records (for births and deaths) to some degree, while 37 states have installed the EVVE vital events network that enables interstate queries; another 11 are in the process of installing EVVE or a similar program; but only five motor vehicle agencies intend to check vital records prior to issuing a driver's license;

  - 32 are issuing their cards from secure or central locations and another five are now switching to central issuance;

  - 38 have installed facial recognition software to help reduce fraud and support law enforcement and another six are implementing it now; this technology is expensive and not required by REAL ID but helps states achieve the "one driver/one license" rule of REAL ID.

- Only three jurisdictions are not significantly improving their license issuance, and two of those are territories.

- These improvements and work toward compliance have occurred despite at least 16 state statutes impeding full compliance with the REAL ID Act.

To be clear, this report is not meant as a substitute for a Department of Homeland Security (DHS) REAL ID Program Office audit. In the autumn of 2008, the DHS Screening Coordination Office produced an extensive 60-page "Concept of Operations" for the REAL ID Program Office "designed to inform DHS senior and executive decision-makers responsible for DHS investment decisions ... and the information to decide how the agency will comply with the statutory mandates of the REAL ID Act." Within the document was a 20-page plan outlining how the office would conduct "State Compliance and Conformity Assessments" to help assure that minimum driver's license issuance standards would be met in an equal and fair manner for the "240 million holders of state driver's licenses and identification cards ... and 675 million U.S. commercial airline travelers" and "56 jurisdictions ... and 2,500 DMV offices and facilities employing about 30,000 employees and contractors." The report was ignored.

The states contacted for this report said they no longer have any guidance or support from DHS in implementing REAL ID. While five states submitted REAL ID compliance packages last year, none of them has been reported out on or deemed compliant by DHS. As a result, no other state that I am aware of has submitted compliance materials since.

Despite the lack of leadership or support by DHS, states have found their way to implement REAL ID standards using some federal funds, but primarily their own budget resources; this is due to the tremendous efficiencies, customer service improvements, anti-fraud, and law enforcement-supportive results that REAL ID minimum standards have created. States have done this despite a national anti-REAL ID campaign by the ACLU and the Cato Institute, despite DHS Secretary Janet Napolitano's failed attempt to repeal REAL ID, and despite legislation in 16 states that hinders full REAL ID compliance. The states with anti-REAL ID legislation either have in some cases barely improved their license issuance, such as Louisiana, or done so significantly by simply stating their improvements meet AAMVA standards (which are more stringent in many cases), not REAL ID standards. States

like Hawaii and Maryland only truly embraced REAL ID relatively recently and are rushing to improve issuance under REAL ID guidelines, while states like Alaska are moving slowly, but still moving toward more secure standards in their unique circumstances.

The island territories (American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and U.S. Virgin Islands) are all in different positions with regard to REAL ID. While Puerto Rico and American Samoa have decided that REAL ID standards are worthwhile, the remaining territories are less than enthusiastic; most of these populations already have passports to pass through security and to present at airline ticket counters, so from a consumer point of view, REAL ID is not essential. However, Puerto Rico has an infamous problem with fake birth certificates being used in the United States for driver's licenses. American Samoa has a mixed native and non-American transient population. Thus, Puerto Rico's and American Samoa's reasons for implementing REAL ID have less to do with boarding planes than with assuring their licenses are not obtained fraudulently or used for nefarious purposes.

REAL ID Implementation Chart Analysis

Below is an explanation and analysis of the core of this annual report, the REAL ID Implementation Chart [link]. An explanation is provided by category. Thoroughly revamped and revetted from last year, this year's chart is updated to provide the most essential information in a user-friendly format. The goal is to provide a visual assessment of how well the country is doing in implementing REAL ID and improving driver's license security across a number of key categories: identity vetting and protection, tamper resistant cards, and secure card production. Each of these areas is complicated and requires a technical understanding of how secure driver's license issuance is achieved. The chart is intended to streamline that process by providing information clearly and succinctly, supported by verified data, so that states, Congress, and other interested parties can find out the basics about the current status of implementation quickly and easily.

The remainder of this report is an explanation of the chart, providing additional facts and anecdotes on state activity in each category. The number headings in the text below refer to the numbered column in the table. All in all, for the second year in a row, it is clear that all jurisdictions are making significant progress on improving their issuance processes and producing more secure credentials. What is new this year is how the technologies that support secure credentialing have taken off in many states, despite their cost outrunning the likely cost of simply implementing the minimum standards required by REAL ID. As a nation, in driver's license issuance, achieving the overall goal of the 9/11 Commission and REAL ID is in sight: to make it extremely difficult for the varieties of driver's license issuance fraud to permeate state motor vehicle issuance departments. By the deadline of January 13, 2013, most states will be substantially or materially or fully compliant with REAL ID. No one would have predicted that five years ago.

1. REAL ID Compliance by January 15, 2013

^ **REAL ID Compliance**. As of April 2011, five states submitted REAL ID full compliance packages to the Department of Homeland Security; no newer data is available from that source. Regulation requires that these compliance packages include "a certification by the highest level Executive official in the state" responsible for overseeing its motor vehicle department that the state "has implemented a program for issuing driver's licenses and identification cards in compliance with the requirements of the REAL ID Act of 2005, as further defined in 6 CFR part 37, and intends to remain in compliance with these regulations." This section of the Final Rule also requires a certification from the state's attorney general that the implementation of REAL ID is authorized by state law; a detailed security plan to protect data and privacy; and a description of the state's exception and waiver processes for incidents when REAL ID requirements do not apply.

The April 2011 compliance information I received from a reliable DHS source and published at that time showed that 41 states had embraced REAL ID tenets.[1] Not privy to internal DHS documents, I have no information on whether any other states have submitted compliance packages since, although it is likely that as the January 15, 2013, deadline looms, some states will choose to do so. Nor am I in a position to determine whether state assertions about compliance or assertions about meeting the 39 individual REAL ID "benchmarks" are accurate. Instead, I have focused on what states are saying and doing in regard to implementing the first 18 benchmarks because that is what states are focusing on currently. I have also had to rely on states' self-assessments as to whether benchmarks are met.

To build the chart, a wide variety of sources were consulted, including but not limited to:

- Publicly available information from DMV websites;
- American Association of Motor Vehicle Administrators (AAMVA) materials, the entity responsible for promulgating and supporting states in license credentialing;
- National Association for Public Health Statistics and Information Systems (NAPHSIS) materials, emails, and conversations on vital record digitization implementation;
- State statutes, budget reports, technology contracts, and policy statements by officials;
- Internal DHS reports;
- Vendor materials publicly available;
- News articles;
- Phone calls to about half the DMV Directors and customer service lines;
- Review of this report prior to publication by a few key stakeholders.

While the data in the chart have been checked and rechecked as thoroughly as possible under the circumstances, there is the possibility for error. Suggestions for corrections from state motor vehicle departments are welcome. Please note that this report is not determining, for example, whether the elements that are required for a "tamper resistant ID" have been incorporated into new card production to make it wholly compliant with REAL ID. Instead, the standard for a check mark on this chart is advertising by the state of new technology in the cards, vendor materials, contracts, budgets, and conversations with a state agency. The goal is to identify attempts and successes in making improvements in driver's license security and identity theft protection that align with REAL ID intent, rather than a technical determination of compliance.

On the categories in the chart pertaining to determination of legal presence through the Systematic Alien Verification for Entitlements (SAVE) database and Social Security Online Verification (SSOLV), AAMVA provides updates that were cross-checked with state "driver's license identification requirement" standards, as well as through phone calls. For example, many states are advertising their switch to central issuance because it directly affects their customers, as do changes in card format. Central issuance affects customers in that they no longer obtain their licenses as they wait or the same day, but receive them later in the mail; states do outreach to limit discontent among residents. Many states have web pages dedicated to tamper-resistant cards, central issuance, and even legal presence requirements and facial recognition. Information contained here on facial recognition and biometric capture was gathered using AAMVA data in a variety of forms, along with vendor information and phone calls.

★★ As of April 2011, four states (Alabama, Florida, Indiana, and Utah) were issuing "Gold Star" driver's licenses that enable residents to use that license as identification for federal purposes to enter a secure facility or commercial

airport prior to the 2014 and 2017 deadlines for individual compliance with REAL ID. As of January 2012, four more states are issuing "Gold Star" licenses: Connecticut, Delaware, South Dakota, and West Virginia. Ohio's "material compliance Gold Star" production will be switched to a REAL ID "full compliance Gold Star" on the full compliance deadline of January 15, 2013.

These states are accompanying their REAL ID-compliant driver's licenses with detailed press releases that make sure customers know of the new cards' availability, what documentation is needed to acquire one, the purpose of the cards, and how they differ from a regular driver's license or ID issued by the state. Each state is providing a name for its REAL ID-compliant card. Each state's card will look different. Yet all of them will have a gold star printed on the licenses to enable Transportation Security Administration (TSA) workers, and other federal security, to easily tell a compliant card from a non-compliant card come 2014 and 2017, when deadlines for Gold Star card-carrying occur.

Last fall, Alabama posted this explanation of its new "STAR I.D." on its website:

> "'In response to acts of terrorism committed against the United States, and in an effort to ensure the safety of citizens, Congress pass the REAL-ID Act of 2005. To comply with the act, the Alabama Department of Public Safety has developed a driver license and identification program called STAR I.D.'
>
> "'Secure, Trusted, And Reliable,' STAR I.D. will be available at Driver's license examining offices in Montgomery, Autauga, and Chilton counties as part of a pilot project that begins Oct. 3, with a statewide launch set to follow after the first of the year.
>
> "All current Alabama driver's licenses and non-driver ID cards will be accepted for official federal purposes until Dec. 1, 2014. Beginning on that date, however, individuals born after Dec. 1, 1964, will be required to have a REAL-ID compliant document to board a domestic flight or gain access to certain federal facilities that require identification. On Dec. 1, 2017, individuals born on or before Dec. 1, 1964, will be required to be in compliance."[2]

Connecticut describes its gold star compliance as "SelectCT ID."[3] Its roll-out includes the following description that discusses both 9/11 and identity protection differently from Alabama, avoiding reference to REAL ID:

> "The Connecticut Department of Motor Vehicles in October will start a new program to offer verified identity protection to people renewing driver's licenses and DMV-issued identification cards. This verification is done now on applicants for new licenses and ID cards. The department will ask renewing customers whether they want to show original identity documents to establish a record of their identity with the agency as well as for federal identification purposes. Customers can also reject the verification and simply get a regular driver's license or ID card.
>
> "Through the program, called SelectCT ID, people verifying will get a gold star on the license or ID card. Those declining will have one stamped "Not for Federal Identification." The difference could be extra screening under a proposed federal program slated to go into effect in 2017 for airports and federal buildings and also use for possible commercial transactions. The program stems from national security measures and federal identification standards resulting from the September 11, 2001, terrorist attacks in the United States. It is also designed to offer residents additional protection against identity theft by having a historical record of proven original identity documents shown to DMV."

Ohio is in the process of beginning production of its "SAFE ID" and uses a "FAQ" section to describe the new card, referencing the requirements as stemming from 9/11 Commission recommendations:

> "Beginning early January 2013, the BMV will issue SAFE ID driver licenses (DL) and identification cards (ID). This means that Ohio has met standards set forth by the U.S. Department of Homeland Security for issuing secure identification documents... SAFE ID refers to a State of Ohio driver license (DL) or

identification card (ID) that is in compliance with the Federal REAL ID Act of 2005. The 9/11 Commission recommended that the U.S. improve its system for issuing secure identification documents. Congress responded to this recommendation by passing the REAL ID Act."[4]

★ As of April 2011, only seven states were meeting the 18 material compliance REAL ID benchmarks. As of January 2012, 27 are meeting, or attempting to substantially meet, these material compliance benchmarks. These compliance determinations are an attempt to discern upgrades to systems since April 2011, when I received an internal DHS document on states' self-assessments on REAL ID compliance. States embracing the standards set forth by REAL ID and going beyond those requirements with additional security measures in processing and biometrics, and are seeking to comply by the January 2013 deadline, were entered into this category.

EDLs are enhanced driver's licenses that meet most of the REAL ID standards and are used by border states to enable their citizens to cross the border without a passport. Only four states on the Canadian border are currently issuing EDLs, with Minnesota set to begin production shortly.

+ In April 2011, 12 states had made improvements in driver's license standards, having met at least 15 of the 18 benchmarks. As of January 2012, the number in this category has dropped to seven, as five states have moved into the material compliance category within the past year.

REAL ID standards were a lower, more generalized standard than the post-9/11 AAMVA standards. Thus even where states do not embrace REAL ID, if they are working on pilots and using AMMVA best practices, they could well now or in the future exceed REAL ID standards. That is the case already with 38 states conducting facial recognition, at least partially, in the area of identity verification.

All these improvements are being made despite 16 states having some form of legislation that prevents full compliance with either the REAL ID Act of 2005 as a whole, or some portion of it, such as laws in Washington and New Mexico not requiring verification of legal presence, which is key to REAL ID compliance. The Alaska legislature will not permit an appropriation to enable legal presence checks. States like Missouri and Montana have outright bans on REAL ID compliance, but even these states are improving standards. Oregon will not permit its motor vehicle agency to share data with other states. Other states, like New Hampshire, cannot spend money on REAL ID compliance without prior approval.

/ In April 2011, 12 states had not pursued any real improvement in driver's license standards or issuance procedures related to REAL ID. That number is now lower, and may only include Louisiana and two territories, Guam and the Marianas. Even Louisiana, however, while steadfastly uninterested in REAL ID, is interested in analyzing its vulnerabilities and working with AAMVA on improvements and access to legal-status verification, as legal presence is important to the state. Alaska was potentially in this category, having met only seven benchmarks, but that's up from fewer than four benchmarks last April, and it has issued requests for contracts on central issuance and facial recognition, putting it at the bottom of the "+" category on this chart, along with the U.S. Virgin Islands.

Key Elements to REAL ID Compliance

The core security mission of REAL ID can be summed up in three areas:

- cards that are extremely difficult to tamper or counterfeit — column 2 in the table;
- verifying and protecting identity and assuring that those that apply are entitled to the driver's license — columns 3, 4, and 5 in the table; and
- secure card production — columns 6 and 7 in the table

2. Tamper-Resistant Cards

A lost or stolen driver's license or ID in the past was a boon to counterfeiters and identity thieves because the cards could be easily modified to a new or assumed identity. Tamper-resistant cards prevent that. The REAL ID Final Rule[5] delineates the following:

> "§ 37.15 Physical security features for the driver's license or identification card.
>
> (a) General. States must include document security features on REAL ID driver's licenses and identification cards designed to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards in accordance with this section.
>
> (1) These features must not be capable of being reproduced using technologies that are commonly used and made available to the general public.
> (2) The proposed card solution must contain a well-designed, balanced set of features that are effectively combined and provide multiple layers of security. States must describe these document security features in their security plans pursuant to §37.41.
>
> (b) Integrated security features. REAL ID driver's licenses and identification cards must contain at least three levels of integrated security features that provide the maximum resistance to persons' efforts to —
>
> (1) Counterfeit, alter, simulate, or reproduce a genuine document;
> (2) Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder;
> (3) Substitute or alter the original or lawful card holder's photograph and/or signature by any means; and
> (4) Create a fraudulent document using components from legitimate driver's licenses or identification cards.
>
> (c) Security features to detect false cards. States must employ security features to detect false cards for each of the following three levels:
>
> (1) Level 1. Cursory examination, without tools or aids involving easily identifiable visual or tactile features, for rapid inspection at point of usage.
> (2) Level 2. Examination by trained inspectors with simple equipment.
> (3) Level 3. Inspection by forensic specialists."

New Jersey's list of 25 REAL ID Card Requirements shows how states technically seek to achieve tamper-resistant cards.[6]

While impossible to know whether every state has incorporated all elements of a secure driver's license/identification as required by the Final Rule — only a DHS audit could produce that information — it is possible to know whether states have made their cards more tamper-resistant. Because the new card "look" directly affects consumers, most states advertise their new designs in varying detail. As of January 2012, at least 43 states were advertising or making information available indicating a variety of improvements in developing tamper resistant cards. Two more are beginning production soon. The remaining 11 either have not or it is unclear.

3. Verification of Social Security Number

The 50 states plus the District of Columbia are actively checking SSNs, while the five territories are working with AAMVA on a pilot that will make SSOLV and SAVE available through both secure web services and a dedicated website that includes an "immigration photo capability." AAMVA was also piloting integration of the deployment of

US PASS, which provides passport data for U.S. citizens, into the DMV check via this same web service. American Samoa is adding US PASS now, the first jurisdiction to do so. US PASS acts as another form of a legal presence check. The jurisdictions committed or interested in AAMVA's web project as of late September 2011 were: Alaska, American Samoa, Connecticut, Delaware, Guam, Florida, Hawaii, Indiana, Iowa, Kansas, Louisiana, Mississippi, Missouri, Nebraska, New Jersey, New Mexico, North Carolina, N. Mariana Islands, Puerto Rico, Texas, U.S. Virgin Islands, and Virginia.

4. Verification of Legal Presence in the United States

Forty-seven jurisdictions are registered with DHS to check legal presence through the database Systematic Alien Verification for Entitlements (SAVE) system, maintained by the federal government to determine legal status for a variety of programs. Two more jurisdictions are coming online, and seven are not. According to USCIS, as of August 2011, DMVs collectively had conducted over 1.9 million queries of SAVE in FY 2011.

Montana is the most recent signatory with U.S. Citizenship and Immigration Services (USCIS) to query SAVE. In April 2011, Montana's legislature passed into law a bill enabling the state to query legal status with the federal government.[7] That law passed by a two-to-one margin in the same legislature that four years earlier rejected compliance with REAL ID by a vote of 150-0 at a time when the governor was one of the most vocal critics of REAL ID.

New Hampshire is set to sign the SAVE Memorandum of Agreement (MOA). At least three of the seven are prohibited or prevented: Alaska, New Mexico, and Washington State. However, as New Mexico pushes to incorporate legal presence into DMV checks anyway, the state recently signed a MOA with USCIS, the agency that maintains SAVE, to link their DMV to SAVE.

Maine's Gov. John Balducci issued this statement in June 2009 upon vetoing a bill that would have repealed legal presence requirements:

> "Forty-six states, including every state in New England, have a legal presence requirement for its credentials. Before last year's actions to increase the security of State credentials, Maine had become a target for unscrupulous individuals looking to circumvent legal presence requirements in other states. People were trucked in, in some cases by van load, to get driver's licenses that would help them break the law elsewhere. With the protections put in place [by Maine Revised Statute Title 29-A, Section 1410.8,9] last year, such activities are much more difficult."[8]

5. Verification of Birth Through the Digitized EVVE Network

Electronic Verification of Vital Events (EVVE). The EVVE network permits queries of in-state and out-of-state vital records for first-time applicants and others. The non-profit National Association of Public Health Information Systems (NAPHSIS) develops, maintains, and installs EVVE in willing states with the support of federal funding through the REAL ID Act. Some initial monies also came from the Kentucky Transportation Cabinet that piloted EVVE. This funding runs out in June 2012. As of February 1, 2012, the vital records agencies in 37 states were online with the EVVE system, and 11 other vital records agencies are in the process of having EVVE installed. The EVVE system is dependent on vital events (births and deaths) being entered into the system by states' vital records agencies in a standard manner so queries can be made both between a state's own agencies and across state lines, and also so the system can provide information to the Social Security Administration and the State Department, both of which are current users of EVVE for SSN and passport applicants, respectively.

States vary in how far back they digitize data, but every state has digitized a significant amount of data. (EVVE recommends that states digitize vital events back to 1945.) Such data provide an opportunity to ensure that first-time applicants and first-time renewals for driver's licenses and identification cards are indeed who they say they are, preventing the most insidious type of identity fraud whereby an entire identity is assumed by someone else for nefarious purposes. Yet no state motor vehicle agency is using EVVE now. The best news is that Delaware, Indiana, Michigan, and Virginia (came online with EVVE on February 18, 2012) intend to begin incorporating EVVE into their identity vetting/anti-fraud procedures for license issuance as soon as possible. American Samoa is currently digitizing its records in accord with NAPHSIS guidelines, and will digitally check birth records at their sole DMV location, but has no plans now to incorporate EVVE.

REAL ID regulations at 6 CFR 37.13(b)(3) strongly recommend that states electronically verify dates of birth provided by applicants:

> "States must verify birth certificates presented by applicants. States should use the Electronic Verification of Vital Events (EVVE) system or other electronic systems whenever the records are available. If the document does not appear authentic upon inspection or data does not match and the use of exceptions process is not warranted in the situation, the State must not issue a REAL ID driver's license or identification card to the applicant until the information verifies, and should refer the person to the issuing office for resolution."[9]

EVVE provides the interstate network and standardization in a dynamic manner, meaning that as states and territories get online with EVVE, states within the program will be automatically connected to the new states, provided agreement by the state holding the records. Like all other queries, the querying state would not have access to the actual data, only a yes/no on a match.

Failure to link to EVVE remains the most essential missing element to REAL ID compliance, not only because the law strongly encourages a digital vital record check, but also because it is the only means of ensuring that a first-time applicant or first-time renewal is presenting a wholly legitimate identity. Facial recognition is extremely good at catching fraudsters and criminals the second time they hit the system, but not the first; only EVVE can do that.

Checking vital events was the key to catching an illegal alien who had assumed the identity of a murdered Ohio boy. In 2010, a Bulgarian who had managed to obtain naturalization and work as an Oregon liquor enforcement agent was caught by the State Department when he applied for a U.S. passport.[10] A Davidson College drop-out, immigration did not catch Doitchin Krastev, despite the fact that the stolen identity had been used since the mid-1990s. Immigration adjudicators even granted him U.S. citizenship. The DMVs where he was issued driver's licenses did not catch him — probably Colorado and/or Oregon. However, the State Department did because State checks vital records in cases of suspected fraud in passport applications. In these situations, EVVE is supposed to be queried as part of State's routine anti-fraud check. If State were not routinely checking vital events, Krastev might well have obtained a passport. Every single driver's license in the United States being issued or renewed is subject to the same possible fraud because states are not routinely checking EVVE.

Complicated cost estimates provided by EVVE for this project compared with research on New Jersey budget and license issuance show that in a state like New Jersey — a mid-sized state — the cost would be about $2 million per year to check all incoming driver's license/identification card applicants name and date of birth against digitized vital records through EVVE. Considering national figures on fraud and DMV identity theft, EVVE estimated that this figure translates into it costing the state of New Jersey about a $1.29 per query. That cost is higher in New Jersey because the DMV's sister vital records agency charges for queries from other agencies in the same state (not all states do) and because no other states are conducting queries. The more states connected to EVVE, the less the nonprofit NAPHSIS must charge to maintain its system.

If all states were on board the cost would be reduced to $0.95 per query. Yet the major cost is not EVVE. If all state vital records offices waived their portion of the fee to state motor vehicle agencies, the cost to run EVVE checks

Driver's License Security Implementation: System Connectivity and Grant Allocation by Jurisdiction (Notes or

	1	2	3	4
Jurisdiction[1]	**REAL ID Compliance by Jan. 15, 2013 (all enrolled by 2017) [2]**	**REAL ID Tamper-Resistant DL/IDs Issued[3]**	**REAL ID SSOLV (SSN Check)[4]**	**REAL ID SAVE (legal presence check)[5]**
Alabama	★★	✓	✓	✓
Alaska	+ –	✓	✓	
American Samoa	★	✓	+	(US PASS)
Arizona	+ –		✓	✓
Arkansas	★	✓	✓	✓
California	+	✓	✓	✓
Colorado	+	✓	✓	✓
Connecticut	^ ★★	✓	✓	✓
Delaware	^ ★★	✓	✓	✓
District of Columbia	★		✓	✓
Florida	★★	✓	✓	✓
Georgia	★	✓	✓	✓
Guam	+		+	+
Hawaii	★	✓	✓	✓
Idaho	+ –	✓	✓	✓
Illinois	★	✓	✓	✓
Indiana	★★	✓	✓	✓
Iowa	★	✓	✓	✓
Kansas	★	✓	✓	✓
Kentucky	★	✓	✓	✓
Louisiana	/ –		✓	✓
Maine	+ –	✓	✓	✓
Maryland	^ ★	✓	✓	✓
Massachusetts	+	✓	✓	
Michigan	★ (for EDLs)	✓	✓	✓
Minnesota	+ (to issue EDLs)		✓	
Mississippi	★	✓	✓	✓
Missouri	+ –	✓	✓	✓
Montana	+ –		✓	✓
Nebraska	★	✓	✓	✓
Nevada	★	✓	✓	✓
New Hampshire	+ –	✓	✓	+
New Jersey	★	✓	✓	✓
New Mexico	+ –		✓	✓
New York	★ (for EDLs)	✓	✓	✓
North Carolina	+	✓	✓	✓
North Dakota	★	✓	✓	✓
Northern Mariana Islands	+	+	+	
Ohio	★★	✓	✓	✓
Oklahoma	+ –	✓	✓	
Oregon	★ –	✓	✓	✓
Pennsylvania	+		✓	✓
Puerto Rico	★	✓	+	✓
Rhode Island	★	✓	✓	✓
South Carolina	+ –	✓	✓	✓
South Dakota	^ ★★	✓	✓	✓
Tennessee	^ ★	✓	✓	✓
Texas	★	✓	✓	✓
US Virgin Islands	+		+	(St. Croix only)
Utah	★★ –	✓	✓	✓
Vermont	★ (for EDLs)		✓	✓
Virginia	★	✓	✓	✓
Washington	★ (for EDLs) –		✓	
West Virginia	★★	+	✓	✓
Wisconsin	★	✓	✓	✓
Wyoming	★	✓	✓	✓

n next page)

5 REAL ID EVVE (interstate network to connect digitized vital records) [6]	6 Central or Secure Issuance[7]	7 Biometric Verification (Facial Recognition and/or Fingerprint)[8]	8 TOTAL Grant Allocation FY08-FY11 (includes money for MI/MO state-to-state license check system development) [9]
✓	✓	✓	$3,188,319
✓ (partial)	+	+	$1,156,393
✓ (partial) +	✓	+ *	$2,108,270
✓			$5,859,429
✓	✓	✓*	$3,149,613
✓	✓	*	$8,018,149
✓	✓	✓*	$3,427,404
✓		✓	$4,159,572
✓ +		✓	$2,308,270
✓			$2,308,270
✓ (partial)	✓	✓	$8,569,075
✓	+	✓*	$5,616,362
✓			$2,108,270
✓	✓	✓*	$2,727,726
	✓	✓	$2,257,726
	✓	✓*	$8,638,857
✓ +	✓	✓	$6,287,956
✓	✓	✓	$3,469,052
✓	✓	✓	$3,182,752
✓		✓	$3,260,813
✓			$3,138,319
	✓		$3,281,637
✓		+	$3,395,726
✓ (partial)	✓	✓	$4,747,954
✓	✓		$5,633,319
✓	✓	+	$2,151,109
✓		✓*	$20,068,535
✓		✓	$2,991,634
✓	✓	✓	$1,156,393
✓	✓	✓	$2,944,914
✓ (partial)	✓	✓	$5,151,333
	✓		$2,257,726
✓	+	✓	$4,425,808
✓ (partial)		✓	$2,757,726
✓ (NYC only)	✓	✓	$7,073,897
✓ (partial)	✓	✓	$4,937,319
✓		✓	$2,308,270
✓			$1,808,270
✓	+	+	$4,338,319
✓		✓*	$1,457,049
✓	✓	✓	$3,427,404
✓	✓	✓	$5,181,119
			$2,108,270
✓	✓	✓	$2,308,270
✓(partial)		✓	$2,757,726
✓		✓	$2,108,270
✓ partial)	✓	✓	$2,951,786
	✓	✓*	$8,018,149
✓ (partial)			$2,108,270
✓	✓	✓	$3,264,144
✓		+	$1,858,270
✓+	✓	✓	$5,798,571
	✓	✓ for EDL only	$3,138,319
✓	✓	✓*	$2,757,727
	✓	✓	$4,328,790
✓ (partial)	+		$2,308,270

Missouri

Driver's License Security Implementation: Notes

[1] **Jurisdiction.** The text of the REAL ID Act is available at http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/html/PLAW-109publ13.htm. The text of the REAL ID Final Rule is available at http://www.uscis.gov/ilink/docView/6CFR/.

[2] **Compliance.** Legal requirements: REAL ID Act 202(d)(11)(B) and 6 C.F.R. 37.17(n)
★ ★ Is or will be issuing 'Gold Star' DLs for use at secure facilities
★ Substantially met or committed to meet 18 benchmarks or more REAL ID requirements
+ improving secure DL/ID standards
– anti-REAL ID legislation
/ Not interested in compliance
^ Submitted compliance package to Department of Homeland Security.

[3] **Tamper-ResistantDL/IDs Issued.** REAL ID Act 202(b)(8). Final Rule provides description in 6 C.F.R. 37.15 for"balanced features to provide multiple layers of security"
+ In process of or intends to issue more secure DL/IDs.

[4] **SSOLV(SSN check)**. REAL ID Act 202(d)(5). Final Rule requires use of SSOLV or "approved method" at 6 C.F.R. 37.13(b)(2).
+ In process of or intends to check SSNs.

[5] **REAL ID SAVE (legal presence check).** Reflects a signed agreement to use SAVE; complete data on actual use unavailable but near all do check). REAL ID Act 202(c)(3)(C). Final Rule requires use of SAVE at 6 C.F.R. 37.13(b)(1)
+ In process of or intends to check legal presence
* Interested in pilot for SSOLV, SAVE and US PASS available via Internet.

[6] **REAL ID EVVE (interstate network to connect digitized vital records).** REAL ID Act Final Rule recommends use of EVVE at 6 C.F.R. 37.13(b)(3). No DMV checks EVVE records; all states digitized, even if not complete for federal purposes. Assures first time applicant identity.
+ Intends to link to EVVE or otherwise conduct vital record checks.

[7] **Central or Secure Issuance.** REAL ID Act 202(d)(7). 6 C.F.R. 37.43(a) requires a secure process; central issuance a best practice.
+ In process or intends to move to central issuance.

[8] **Biometric Verification..** REAL ID Act does not require biometric verification but supports identity verification at Final Rule 6 C.F.R. 37.13. Assures applicant identity protected, not misused.
* Biometric capture
+ In process or intends to use facial recognition.

[9] **TOTAL Grant Allocation FY08-FY11.** $221.36 million cumulative total 2008-2011. FY11 allocation is $44,910,000. FY11 Homeland Security Grant monies allocation by FEMA deleted requirement that REAL ID monies be used only for REAL ID compliance, and instead the allocation reads as follows: "to prevent terrorism, reduce fraud and improve the reliability and accuracy of personal identification documents that states and territories issue."

would be reduced to $.08 per transaction, which is doable. (A few states have laws preventing data sharing and would require legislation to permit EVVE interstate data sharing. However, these laws should not prevent intrastate sharing of vital event information, which accounts for a large majority of queries in states.)

The issue is not the non-profit network provided by NAPHSIS for interstate queries, but the cost of maintaining up-to-date state and local vital records offices. It is the fees charged by state vital records agencies for sharing vital events records that truly needs to be addressed, which would likely require legislation or regulation. While the REAL ID Final Rule has been amended, those amendments only pertain to deadlines for compliance; vital events would likely not be a priority. In addition, it is highly unlikely that any proposed REAL ID vital events regulation would go so far as to promulgate standards beyond the "paper" version of vital events, namely, birth and death certificates.

Birth Certificate Standardization. While REAL ID strongly recommends use of EVVE, it does not require its use to verify birth information. Instead, states may rely on birth certificates. Yet the birth certificate is the easiest of all records to counterfeit today, with no standardization of issuance, nor control in most states at the state level on issuance; every jurisdiction produces its own brand of birth certificate. The 9/11 Commission recommended standardization, and the REAL ID Act required it, but regulations drafted seven years ago remain unpublished.

While these regulations remain in a lock box, any regulation would have to address the actual security of the paper birth certificate as well as eliminate inconsistencies and help ensure uniformity across the birth certificate issuance spectrum. As is, it is impossible to tell a fake from real birth certificate. New regulations would also have to ensure consistent minimum issuance costs for jurisdictions that may find, like motor vehicle departments nationwide, that the new standards will not only add security but also create efficiencies and maintain or reduce cost over time.

6. Secure Production and Central Issuance

REAL ID requires either secure over-the-counter processes and procedures for issuing and producing the cards, or the recommended best practice of "central issuance," whereby the applicant applies at a local DMV counter for the license, and it is mailed from a central facility in 15 to 30 days. REAL ID provides leeway in defining "secure production," as many states with over-the-counter issuance were concerned about significant cost to revamp to central issuance. The REAL ID regulation at 6 CFR 37.43(a) specifies that "States must ensure the physical security of facilities where driver's licenses and identification cards are produced, and the security of document materials and papers from which driver's licenses and identification cards are produced or manufactured."[11] Each state is to "describe the security of DMV facilities as part of their security plan." Central issuance is considered a best practice as it ensures only cleared personnel have access to private data and manufacturing products for cards, and the facilities themselves are not susceptible to theft or fraud.

Most states combine central issuance with facial recognition, running facial recognition after an application has been submitted in a non-rushed manner against other digital photos in their system to determine fraud or other criminal activity. (See more on facial recognition below.) If there is no fraud, the secure facility mails the securely produced card to the applicant. Otherwise it is not issued until after an investigation.

More than 20 states employed central issuance prior to REAL ID becoming law. Today, 32 states have fully implemented central issuance, five are in process, and 19 have not. As an example of cost breakdowns, New Jersey signed its seven-year contract with the major driver's license vendor, L-1 Identity Solutions, for a combination over-the-counter enhanced image-capture ($5,983,000), facial recognition hardware and software ($4,220,000), central issuance ($841,500), and facial recognition "scrub" of all current license holders ($185,000), for a total of $11,229,500.

In my analysis last year, I concluded that REAL ID compliance per state would cost on average twice what the federal government had already allocated.[12] Under that assessment, New Jersey's REAL ID compliance costs would

be about $7 million, substantially less than what the state has decided on its own to pay for the immense anti-fraud benefits that technologies like facial recognition, image scrubs, and enhanced photos bring to driver's license issuance that are not required by REAL ID, but support its intent of thorough identity vetting.

Arkansas is one of the few states on the list that does over-the-counter "while you wait" issuance, but is also one of the few states that does both a "photo first" check before the application is considered and one-to-one facial match (image run against other images with same identity information as applicant's) before issuance. Arkansas then does a "one-to-many" check (digital image run against entire database of archived digital images) by batch at night. Thus, Arkansas is securing the issuance to the person who has been issued a prior card with the same information. The only issue is that without conducting the one-to-many check before issuance, if that person has been issued multiple driver's licenses under different names, the individual already has the card in hand when the state finds that out, and then must embark on a difficult revocation process.

Nebraska's Department of Motor Vehicles has combined central issuance with facial recognition. At a June 2011 presentation, Nebraska DMV Director Beverly Neth provided a number of lessons learned and related the tremendous law enforcement and anti-fraud value of running digital images against an entire archive of images before cards are issued from a secure, central facility. Below are summarized findings from her presentation[13]:

- On the first day of central issuance/facial recognition production, "Maria" applied for an ID card. A possible match with "Herlinda's" image was found. Herlinda (the victim) and legal resident of Texas had spent five years trying to resolve an identity theft where the IRS was requesting taxes owed on $120,000 of income. In January 2010, a federal grand jury indicted "Maria."

- Las Vegas Police provided a photo taken by a surveillance camera in a dressing room. The image was scanned to the facial recognition database and a match was found. That match was wanted in connection with several gang-related homicides.

- The U.S. Marshals Office made a request that Nebraska DMV compare a photo from the Utah sex offender registry in its facial recognition software. Nebraska's software matched the Utah sex offender photo to a Nebraska ID holder, who turned out to be the suspect. The suspect had used his brother's personal information to obtain a Nebraska ID card. Suspect was found in Florida and taken into custody.

- Nebraska State Patrol Cyber Crimes Unit provided a photo of a man who was arranging to meet with a "13-year-old girl" (actually a state trooper). Facial recognition matched the photo to a Nebraska license holder and the individual was arrested.

- Of the 165 cases initiated, 40 of them resulted in arrests, 90 percent of whom had prior criminal histories and 50 percent of whom were "related to immigration."

7. Facial Recognition

Facial recognition technologies are not required by REAL ID, but support the overall goal of REAL ID, which is based on the 9/11 Commission finding that a "higher bar" should be set "for determining whether individuals are who or what they claim to be" (Final Report, p. 384). Such technologies also support the AAMVA recommendation that license holders have only one license at a time; they also protect against identity theft at the DMV counter. As of January 2012, 38 states are using facial recognition, six are or will be implementing it, and only 12 have not.

Facial recognition works to ensure that only one license is issued per applicant and can identify those that have acquired multiple licenses under different names. These systems in the past few years have been responsible for catching identity thieves, wanted criminals, and illegal aliens. These systems cost, for example, $3.5 million in Colorado just for upgrades (2012 budget)[14] or $10.4 million in New Jersey (a seven-year contract).[15] However, the

anti-fraud benefits make the cost worthwhile to these states. Current REAL ID appropriations guideline language enables states to use REAL ID federal money to make these upgrades.

Nearly every state that has implemented facial recognition has a multitude of interesting cases of identity thieves caught only because the state began using the technology. Texas provides an example of a state justifying expenditures on DMV improvements in the areas of facial recognition, tamper resistant cards, and protections against internal and external corruption in its Department of Public Safety Director's Strategic Outlook for 2009-2013:

> "To meet the technological needs of the future, the Department continues to enhance the driver's license issuance process through the implementation of current technologies. To address growing issues we face daily regarding identity theft and fraud, the Department's Driver license Reengineering project introduces technology needed to both monitor and audit controls to identify suspicious issuance activity both from external and internal occurrence ... . Upon legislative approval, this project provides the necessary foundation to allow for addressing Federal Real ID requirements. Facial recognition technology will also be introduced to the issuance process with the development of the Image Verification System which will compare the applicant's facial image to the last image on file to prevent identity theft. The technology will allow law enforcement to export photographic images into the system to identify unknown individuals enhancing an investigator's ability to establish new leads. The Department will include many new state-of-the-art card security features that will make alteration and counterfeiting the card extremely difficult to successfully achieve."[16]

Oregon's program in November 2011 hit 1.8 million photos and incidences of potential fraud arose in 940 cases referred to law enforcement.[17] In one incident sent to us by the Oregon DMV, the identity thief, who stole his brother's identity and others, was found guilty of 17 felony counts on other charges and was sentenced to 96 months in prison.

In Kansas, according to a DMV investigator, facial recognition catches "12 to 15 cases of suspected fraud weekly, and since July 2004, has halted approximately 1,200 cases of attempted identity theft and driver's license fraud."[18]

The chart in this report does not include a separate category for "photo first", but Jennifer Cohen, Director of the Delaware Motor Vehicle Division, a state that came into substantial compliance with REAL ID in about a year, wrote this in an e-mail about customer satisfaction and reducing fraud:

> "Implementing the photo-up-front licensing process has been a two-fold success, first it has significantly reduced the risk of fraud as we are able to run the photo through our facial recognition process to ensure the individual is who they say they are before issuing a credential and secondly we have been able to reduce our customer transaction times by 2-3 minutes which speaks volumes about the effectiveness of our new business flow. Our customers expect a minimal wait while they are at our facilities and trust that their information is secure. We have accomplished that in Delaware."

8. Federal Funding to States

States and territories have received $221.36 million in federal grant monies. Prior year allocations are detailed in last year's REAL ID assessment, "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud."[19] This past year, direct funding for driver's licenses was discarded, partly due to rumors that the driver's license funds were not being used by the states. As is clear from the data presented here, almost all states are working hard to improve their driver's license issuance and are likely spending more than any federal grant monies provided. If anything, considering how DHS is currently absent from active support for REAL ID compliance, states have partly given up asking for more federal money, and are working from their own budgets.

Even as states are exceeding REAL ID requirements, improvements in general are not as expensive as assessed years ago. However, most states are spending millions, and usually more than DHS allocates. It's notable that in the FY 2011 allocations below, only $278,000 was returned to the Treasury from FY 2010 allocation to the states of $48,000,000 and available for reallocation in FY 2010. Clearly, the states are using the federal appropriations.

FY 2011 appropriation was $44,910,000 to "reduce fraud and improve the reliability and accuracy of personal identification documents that states and territories issue." Note that REAL ID is not mentioned, nor compliance with REAL ID technical standards referenced. Last year's description by the DHS grant office made no mention of REAL ID except tangentially here:

> "As appropriated by the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112-10) and authorized by Title II of the REAL ID Act of 2005, Division B of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (Public Law 109-13), the FY 2011 DLSGP provides funding available to state driver's licensing authorities (i.e., motor vehicle agencies) for FY 2011 DLSGP related projects. The FY 2011 DLSGP provides funding to prevent terrorism, reduce fraud and improve the reliability and accuracy of personal identification documents that states and territories issue. DLSGP is intended to address a key recommendation of the 9/11 Commission to improve the integrity and security of state-issued driver's licenses (DL) and identification cards (ID).
>
> "Funding
> In FY 2011, the total amount of funds distributed under this grant program was **$45,188,000. All states and territories** that applied for FY 2011 DLSGP **received a base amount, with the balance of grant funds distributed based on the total number of drivers licenses and identification cards (DL/IDs) issued in each state."** [Emphasis added.][20]

The report then goes on to provide line items per jurisdiction that add together the $278,000 left over from FY 2010 and the FY 2011 appropriation of $45,188,000:

Category 1: $1,512,900 each for California, Florida, Illinois, New York, and Texas

Category 2: $979,269 each for Alabama, Arizona, Georgia, Indiana, Louisiana, Massachusetts, Michigan, North Carolina, New Jersey, Ohio, Pennsylvania, Virginia, and Washington.

Category 3: $701,062 each for Arkansas, Colorado, Connecticut, Hawaii, Iowa, Idaho, Kansas, Kentucky, Maryland, Maine, and Minnesota. Missouri and Mississippi, "through the recovery of previous years' funding received [$701,062 + 185,615] and [$701,062 + 92,385], respectively." $701,063 each for Nebraska, New Hampshire, New Mexico, Nevada, Oklahoma, Oregon, South Carolina, Tennessee, Utah, Wisconsin, and West Virginia.

Category 4: $556,393 each for Alaska, American Samoa, District of Columbia, Delaware, Guam, N. Mariana Islands, Montana, North Dakota, Puerto Rico, Rhode Island, South Dakota, U.S. Virgin Islands, Vermont, and Wyoming.

End Notes

[1] See http://www.cis.org/real-id-terrorist-abuse.

[2] http://dps.alabama.gov.

[3] http://www.ct.gov/dmv/cwp/view.asp?a=4078&q=477742.

[4] http://www.ohiobmv.com/Safe_ID_FAQs.pdf.

[5] http://www.uscis.gov/ilink/docView/6CFR/HTML/6CFR/0-0-0-1/0-0-0-4972/0-0-0-5202.html.

[6] https://wwwnet1.state.nj.us/treasury/dpp/ebid/Buyer/GetDocument.aspx?DocId=4172&DocName=09-x-20644Appendix9.pdf.

[7] http://www.cis.org/kephart/montana-real-id-legal-presence.

[8] http://www.maine.gov/tools/whatsnew/index.php?topic=Gov+News&id=74192&v=Article-2006.

[9] http://www.uscis.gov/ilink/docView/6CFR/HTML/6CFR/0-0-0-1/0-0-0-4972/0-0-0-5184.html.

[10] http://www.kval.com/news/local/Deportation-for-Bulgarian-who-stole-dead-boys-ID-worked-for-OLCC-138413294.html.

[11] http://cfr.vlex.com/vid/37-physical-security-dmv-production-289136606.

[12] http://www.cis.org/real-id.

[13] http://www.docstoc.com/docs/82329034/Central-Card-Production-and-Issuance-Process---Lesson-Learned.

[14] http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22Drivers+License+Upgrade+January+2012.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251766806788&ssbinary=true.

[15] http://www.state.nj.us/treasury/purchase/noa/contracts/t2466_09-x-20644.shtml.

[16] http://www.txdps.state.tx.us/dpsStrategicPlan/2009-2013/07directorsstrategicoutlook.pdf.

[17] http://www.oregonlive.com/news-network/index.ssf/2011/11/oregon_dmvs_facial_recognition.html.

[18] http://candaceschuler.com/sites/default/files/portfolio/Case%20Study%20-%20Kansas%20DMV.pdf.

[19] http://cis.org/real-id.

[20] http://www.fema.gov/txt/government/grant/2011/fy11_dlsgp_factsheet.txt.

Backgrounder

REAL ID Implementation Annual Report

Major Progress Made in Securing Driver's License Issuance Against Identity Theft and Fraud

By Janice Kephart

The September 11 hijackers had between them 30 state-issued driver's licenses and non-driver identification cards. These IDs were used not only to board airplanes but also to navigate in our society in preparation for the attacks. This is why the 9/11 Commission recommended a tightening of ID standards and why Congress in 2005 passed the REAL ID Act.

This report is an attempt to provide a comprehensive assessment of how well states are doing in improving driver's license issuance standards of the REAL ID Act. The Act was designed to protect identities and driver's license and identification cards while eliminating fraud and improving the customer experience. REAL ID contains 39 benchmarks; only the most important are covered here, grouped into eight categories, and presented in the chart that forms the heart of this report (see pp. XX).

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185 • (202) 466-8076
center@cis.org • www.cis.org

Support the Center through the Combined Federal Campaign by designating **10298** on the campaign pledge card.

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185
center@cis.org
www.cis.org

NON-PROFIT
U.S. POSTAGE
PAID
PERMIT # 6117
WASHINGTON, DC