AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SECURE IDENTIFICATION: THE REAL ID ACT'S MINIMUM STANDARDS FOR DRIVER'S LICENSES AND IDENTIFICATION CARDS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 21, 2012

Serial No. 112–103

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

73–416 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JARED POLIS, Colorado

RICHARD HERTLING, *Staff Director and Chief Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
MARK AMODEI, Nevada

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
JARED POLIS, Colorado

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 21, 2012

Page

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 3

The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 4

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 5

WITNESSES

David Heyman, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security
Oral Testimony 47
Prepared Statement 49

Darrell Williams, former Senior Director, Office of State-Issued ID Support, U.S. Department of Homeland Security
Oral Testimony 53
Prepared Statement 54

Stewart A. Baker, Partner, Steptoe & Johnson, LLP
Oral Testimony 58
Prepared Statement 59

David Quam, Director, Office of Federal Relations, National Governors Associaton
Oral Testimony 63
Prepared Statement 64

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Material submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 6

Material submitted by the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 10

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the American Civil Liberties Union (ACLU) 81

Letter from Patricia W. Potrezebowski, Ph.D., Executive Director, the National Association for Public Health Statistics and Information (NAPHSIS) . 87

Letter from Brian Schweitzer, Governor, State of Montana 90

Page

Letter from Chuck Canterbury, National President, Fraternal Order of Police 91

Prepared Statement of the National Conference of State Legislatures 93

Prepared Statement of Paul E. Opsommer, State Representative, Michigan House of Representatives, and Chair, Michigan House Transportation Committee 98

Prepared Statement of the North American Security Products Organization (NASPO) 102

SECURE IDENTIFICATION: THE REAL ID ACT'S MINIMUM STANDARDS FOR DRIVER'S LICENSES AND IDENTIFICATION CARDS

WEDNESDAY, MARCH 21, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 9:59 a.m., in room 2141, Rayburn Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Smith, Scott, Conyers, Chu, Deutch, Jackson Lee, and Polis.

Staff present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Andrea Loving, Counsel; Arthur Radford Baker, Counsel; Lindsay Hamilton, Clerk; (Majority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensberger, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will come to order. Today's hearing examines whether the Department of Homeland Security is taking its responsibilities seriously to help ensure that all states and territories have the resources and guidance they need in order to comply with the secure identity document standards put in place by the REAL ID Act of 2005.

I authored REAL ID based on the necessity to help ensure the security of driver's licenses and other state-issued identification cards. Just as the September 11th hijackers exploited loopholes in our U.S. immigration system, they also exploited loopholes in state driver's license systems. The terrorists moved freely throughout our country prior to September 11th. They took flying lessons, purchased airline tickets, rented cars, airplanes and condos. They were able to do these things because, as the 9/11 Commission found, the 19 hijackers had at least 30 pieces of identification, most fraudulently obtained. They ultimately used these identification documents to board the airplanes with which they murdered over 3,000 innocent people.

The September 11th attacks forced us to acknowledge the weaknesses in the driver's licenses and identification document issuance process. At that time, most states did not even verify the true identity of the person before issuing the most universally accepted form of identification in the United States, the driver's license. The 9/11

Commission recognized the importance of secure identification to prevent terrorist activity. They stated that, quote, "Members of al Qaeda clearly valued freedom of movement as critical to their ability to plan and carry out the attacks prior to September 11th," unquote. In addition, the Commission noted that if terrorist travel options are reduced, they may be forced to rely on means of interaction which can be more easily monitored and resort to travel documents that are more easily detectable.

The REAL ID Act established minimum standards for state-issued driver's licenses and identity documents that are used for Federal purposes, such as to enter a Federal building or a nuclear power plant or to board an airplane. States are free to issue and accept non-REAL ID-compliant IDs so long as they are clearly marked "not for identification purposes."

Despite the REAL ID Act's enactment, DHS is hindering implementation by the states. Specifically, I am concerned about the clear lack of commitment by the Department to enforcing the REAL ID standards. Every effort has been made by the Secretary of Homeland Security to create confusion as to whether the law will remain in place.

Secretary Napolitano boldly stated her intent first to repeal REAL ID and then to repeal and replace REAL ID, and she seems now to simply ignore it. DHS has not allocated adequate resources to fully implement REAL ID. The Office of State-Issued Identification Support is within the Office of Policy, which makes little sense, and it doesn't have enough staff to adequately verify compliance packages submitted by the states or to provide adequate guidance to the states regarding compliance. And even more telling is the lack of commitment of the fact that the fiscal year 2012 DHS did not even bother to publish grant guidance or to allocate money for REAL ID grants.

Additionally, I am concerned that DHS has not yet coordinated with the Federal Protective Service, Transportation Security Administration, or any other relevant Federal agency regarding enforcement of the upcoming January 2013 state implementation deadline. It seems that the DHS has not taken any steps to prepare for the deadline or to alert the traveling public regarding the coming deadline.

Despite a lack of guidance and communication from DHS, many states are moving forward with identification security reforms based upon guidance provided by the prior Administration. In fact, according to DHS, six states have submitted full compliance certification packages, 22 other states are materially compliant and are issuing compliant documents or are committed to compliance, 12 states or territories are committed to meeting 15 of the 18 REAL ID benchmarks, and 4 additional states have enhanced driver's license programs comparable to REAL ID guidelines.

States need to understand that the January 2013 deadline will, in fact, be the final deadline. They need to understand that secure identification is a DHS priority, and they need to know that DHS is serious about helping them get to full implementation. I certainly hope that DHS will not abrogate one of its responsibilities to the American people by once again extending the deadline.

It is now my pleasure to recognize for his opening statement the Ranking Member of the Subcommittee, the gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I thank you for convening today's hearing.

While it is a good idea to improve the security of state-issued IDs and driver's licenses, I have some concerns about the implementation of the REAL ID Act. If we make it more difficult for terrorists to get IDs, we also make it more difficult for everybody else. And if the process doesn't actually prevent terrorists from getting an ID, all we have left is the expense and inconvenience for law-abiding citizens.

The REAL ID Act requires tighter standards for driver's licenses and identification cards. It was enacted in response to the 9/11 Commission's recommendation to implement a more secure form of identification for boarding aircraft and accessing vulnerable facilities. These are seemingly prudent and necessary requirements.

The Act, however, has been subject to significant resistance from the states. Prior to the passage of REAL ID, and almost immediately after 9/11, many states were already taking action to tighten driver's licensing standards. Intelligence Reform and Terrorism Prevention Act of 2004 provided for a collaborative rule-making process that included states to achieve these goals. The REAL ID Act interrupted and replaced that process with a more rigid system of requirements that raise a number of budgetary and privacy concerns.

Many elected officials in state governments across the country simply oppose the REAL ID Act on principle. They see it as an unfunded mandate. The REAL ID Act has significant expense. The Department of Homeland Security initially estimated that it would cost over $23 billion for states to implement. The most recent estimate is around $10 billion. But, of course, Congress has appropriated only a fraction of that to defray the costs.

Today, 7 years after the legislation's enactment, 25 states, either through statute or legislative resolution, have rejected the REAL ID Act or said they would simply not comply with it. Especially now, since states face unprecedented budgetary constraints, it is essential that we find cost-effective ways to meet the objectives of the REAL ID Act.

At the same time, privacy and civil rights organizations from across the political spectrum have also objected to the REAL ID. They see the legislation as a de facto national ID card, one that will be used not just for boarding an airplane but ultimately will be required for many other types of transactions, raising significant privacy concerns.

Critics point out that the REAL ID would require a national consolidated driver's license database accessible to thousands of DMV officials across the country. If hacked or otherwise compromised, millions of Americans could be at risk of identity theft.

I am also concerned that the full implementation of the Act would make it more difficult for citizens to vote. According to DHS, final regulations complying with the REAL ID is expected to create a significant expense to citizens as they acquire and pay for necessary documents and wait in long lines at the DMV. In fact, DHS

estimates that Americans will spend hours complying with the Act. All of this is in addition to the direct cost of almost $4 billion imposed on the states, a cost that will be passed on directly to drivers in the form of higher fees.

This money and administrative burden will effectively stand in the way of those trying to vote in states requiring the furnishing of ID by voters, and the burden will fall most heavily on low-income workers without paid vacation or disposable income to spend on new fees.

While we all agree that security and validity of the identification requirements are important issues, there are real problems with implementing REAL ID, and so I look forward to today's hearing to see what the witnesses have to say and how we can comply.

Thank you, Mr. Chairman. I yield back.

Mr. SENSENBRENNER. The Chair recognizes the Chairman of the full committee, the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Last September marked the 10th anniversary of the 9/11 attacks. Unfortunately, a key recommendation of the 9/11 Commission, which called for secure forms of identification, is still not completely addressed, and it seems that this Administration has very little interest in addressing it.

On September 11, 2001, Americans were attacked by foreign nationals who exploited our laws and lived unnoticed in the United States. Nineteen of the hijackers fraudulently obtained 17 driver's licenses from Arizona, California and Florida, and 13 state-issued IDs from Florida, Virginia and Maryland.

During the planning stages of the attacks, these identification documents were used to rent vehicles, evade law enforcement officials, and enroll in flight school. Ultimately, the hijackers showed these licenses and identification cards in order to board the airplanes they used to murder over 3,000 innocent Americans.

Because of these loopholes in our laws, the 9/11 Commission recommended that the, quote, "Federal Government should set standards for the issuance of birth certificates and sources of identification such as driver's licenses," end quote. The Commission went on to state, "Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."

The Commission was correct, and in 2005 Congress passed and the President signed the REAL ID Act into law. This law addresses this security gap and requires states to meet certain security standards for issuance of driver's licenses and identification cards. Despite that action nearly 7 years ago, REAL ID has not yet been fully implemented.

The current Administration has actually undermined the REAL ID Act whenever possible. They extended the compliance deadline two times, most recently in March of last year. Now states do not have to comply with REAL ID until January 15th, 2013, which is 11-and-a-half years after the 9/11 attacks. And Secretary Napolitano has consistently supported the repeal of REAL ID instead of compliance with the law.

Many states understand that they need to issue secure forms of identification. They do not want to issue a driver's license to the next terrorist. Unfortunately, the Department of Homeland Security does not seem to have the resources in place to help ensure that states get the guidance they need in order to comply with REAL ID.

The risk of not implementing REAL ID is great. That is apparent in the facts that surround the February 2011 arrest of Khalid Ali-M Aldawsari in Texas on a Federal charge of attempted use of a weapon of mass destruction. According to the arrest affidavit, when the FBI searched his residence, they found his journal in which he wrote of the need to obtain a forged U.S. birth certificate, multiple driver's licenses, and a U.S. passport. He planned to use those driver's licenses to rent several cars, each with a different license, specifically to avoid detection.

This is evidence that terrorists still plan to exploit the weaknesses in our driver's license issuance processes in order to attack us. If we don't do everything in our power to fully implement REAL ID, we set ourselves up for another attack. History can only repeat itself if we let it.

Thank you, Mr. Chairman. I yield back.

Mr. SENSENBRENNER. Thank you very much.

The Chair recognizes the junior Chairman emeritus, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Sensenbrenner. I am delighted to be here in my relegated capacity to be permitted to make an opening comment.

I notice the impatient tone in the Chairman's voice about the delays that have occurred in terms of the REAL ID Act. But I would like to put forward a bipartisan recognition of some concerns that we have, and they start off with the governor of North Carolina, the former governor of South Carolina, Governor Mark Sanford, who called the REAL ID Act, quote, "the worst piece of legislation I have seen during the 15 years I've been engaged in the political process," end quotation.

And then I call to my colleagues' attention the other 28 organizations and individuals, prominent individuals, including Bob Barr, a former Member of this Committee and chairman of Liberty Guard, who have said that this legislation would harm individual liberty and waste precious taxpayer resources.

Now, that doesn't mean that they are all right and the Chairman is all incorrect. I think, though, we have to take the 28 organizations, the American Civil Liberties Union, the American Library Association, the Asian Law Caucus, the Consumer Federation of America, Consumer Watchdog—I will put all these in—the Hispanic Leadership Conference, and——

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

RE: Coalition Opposes Any Efforts to Force Compliance with Real ID

Dear Representatives

We the undersigned organizations write today to express our opposition to any effort by Congress or the Department of Homeland Security (DHS) to force states to comply with the Real ID Act of 2005. Real ID was passed as a rider to a bill funding military expenditures and tsunami relief. It gave states three years to comply with restrictive federal licensing standards, create a national database of drivers' license information and build huge databases of individual birth certificates and other personal information. All of this would have cost billions – a cost borne almost exclusively by the states.

Instead of compliance, Real ID faced widespread opposition. Groups from across the political spectrum opposed it. Supporters of fiscal conservatism and federalism decried it as an unfunded mandate that trampled on the Tenth Amendment. Civil rights and civil liberties groups worried that the Act lacked sufficient protections and might increase racial discrimination. Defenders of religious freedom described its negative impact on the Amish and other religious denominations. Consumer groups feared it would result in an expansive and cumbersome new bureaucracy. Advocates against domestic violence believed it would expose personal information about survivors of domestic violence and sexual assault.

In addition, many of those same groups rejected Real ID as a national ID. They believed it would facilitate tracking of data on individuals and bring government into the very center of every citizen's life. It would be a de facto government permission slip needed by everyone in order to travel. As happened with Social Security cards decades ago, use of such ID cards would then quickly spread and be used for other purposes – from work to voting to gun ownership.

States rejected Real ID because of its high cost – initially estimated by DHS at $23 billion. States were concerned that the Act would force them to change their entire licensing issuance process to conform to a one-size-fits-all federal mandate. At the same time the states were also making great strides in improving drivers' license security and were rightly concerned that Real ID would interfere with or overturn many of these efforts. Twenty five states, either through a statute or legislative resolution, rejected the Act or said they would not comply with Real ID.[1] Fifteen of those states actually passed laws prohibiting compliance with Real ID.

As a result of this widespread opposition, Real ID has stalled. DHS cannot mandate compliance because implementing its sole penalty under the statute – barring the use of non-compliant licenses for boarding airplanes – would bring air travel to a halt. Nor has Congress acted to fund the legislation. It has provided only $200 million for Real ID compliance, a fraction of the amount needed to comply with the law.

[1] The states are Alaska, Arizona, Arkansas, Colorado, Georgia, Hawaii, Idaho, Illinois, Louisiana, Maine, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, North Dakota, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Virginia and Washington.

Given this reality, any additional Real ID compliance efforts by DHS or Congress would harm individual liberty and waste precious taxpayer resources. The undersigned organizations urge you oppose any efforts to attempt to force compliance with Real ID.

Sincerely,

American Civil Liberties Union

American Library Association

Asian Law Caucus, member of Asian American Center for Advancing Justice

Bob Barr, Former Member of Congress and Chairman of Liberty Guard

Center for Financial Privacy and Human Rights

Constitutional Alliance

Consumer Action

Consumer Federation of America

Consumer Watchdog

Center for Democracy & Technology

Defending Dissent Foundation

DownsizeDC.org, Inc.

5-11 Campaign

Electronic Frontier Foundation

Electronic Privacy Information Center

Floridians Against REAL ID

Hispanic Leadership Fund

The Leadership Conference on Civil and Human Rights

Liberty Coalition

The Multiracial Activist

Patient Privacy Rights

Privacy Activism

Privacy Times

Robert Ellis Smith, Publisher, PRIVACY JOURNAL

The Rutherford Institute

TakeBackWashington.org

Taxpayers Protection Alliance

World Privacy Forum

Mr. CONYERS. I thank the Chair, and let me go directly to what the problem is and what we can do about it.

Number one, I am going to ask the Subcommittee Chair and the Ranking Member to let me join with them in an invitation to Janet Napolitano, our Secretary, and ask that we meet with her as reasonably soon as possible, perhaps before the recess, to see if we can make progress on this issue. She was before the committee, one of

the committees in Judiciary only recently, but this was not the subject of the conversation.

Mr. SENSENBRENNER. If the gentleman will yield.

Mr. CONYERS. Certainly.

Mr. SENSENBRENNER. I would be happy to invite her, and I invite the gentleman from Michigan to help us prod her into following the law that was passed——

Mr. CONYERS. Thank you.

Mr. SENSENBRENNER. I think a long time ago.

Mr. CONYERS. Well, we didn't do it, so let's do it now. But I appreciate the gentleman's cooperation, Chairman.

Then the last two points that I would like to make that get down to what I would like to hear from the witnesses about. The problem with the REAL ID mandate, as Mr. Scott said, it is an unfunded mandate, $23 billion worth of unfunded mandate, and one of the things, if we have such a meeting, Mr. Chairman, would be to figure out how we can really work out the funding of this.

The other issue is the matter of the privacy concerns. States and their citizens are worried about the far-reaching implications of having so much personal information becoming so accessible to so many organizations, state agencies and people. I think there may be ways that could come out of this important hearing to tighten up privacy restrictions and address these concerns in an appropriate way.

And so it is with that spirit of bipartisanship that I look forward to the testimony of our very welcome witnesses. I thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman's time has expired.

I ask unanimous consent to submit for the record materials from the Center for Immigration Studies, the National Association of Public Health Statistics and Information Systems, the Document Security Alliance, and the Coalition for a Secure Driver's License.

And without objection, the Chair will be authorized to declare recesses during votes on the House floor.

Hearing no objection, so ordered.

[The information referred to follows:]

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 56 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 reverted 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.

Center for Immigration Studies

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 Baldacci 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

Center for Immigration Studies

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

Jurisdiction[1]	1 REAL ID Compliance by Jan. 15, 2013 (all enrolled by 2017) [2]	2 REAL ID Tamper-Resistant DL/IDs Issued[3]	3 REAL ID SSOLV (SSN Check)[4]	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	- (for some 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	★	✓	✓	✓

next page)

5 REAL ID EVVE (interstate network to connect digitized vital records) *	6 Central or Secure Issuance*	7 Biometric Verification (Facial Recognition and/or Fingerprint)^	8 TOTAL Grant Allocation FY08-FY11 (includes money for MI/MO state-to-state license check system development) ¶
✓	✓	✓	$5,188,519
✓ (partial)	-	-	$1,150,393
✓ (partial) +	✓	- *	$2,108,270
✓			$5,859,429
✓	✓	✓*	$3,110,613
✓	✓	-	$5,018,149
✓	✓	✓*	$5,427,404
✓		✓	$4,159,576
✓ +		✓	$2,308,270
✓			$2,308,270
✓ (partial)	✓	✓	$8,569,075
✓	-	✓*	$5,616,562
✓			$2,108,270
✓	✓	✓*	$2,757,726
	✓	✓	$2,257,726
	✓	✓*	$8,618,857
✓ +	✓	✓	$6,287,956
✓	✓	✓	$5,460,092
✓	✓	✓	$5,182,752
✓		✓	$5,280,818
✓			$5,138,319
	✓		$5,281,657
✓		-	$5,399,726
✓ (partial)	✓	✓	$4,747,054
✓	✓		$5,633,319
✓	✓	-	$2,151,109
✓		✓*	$20,068,535
✓		✓	$2,991,638
✓	✓	✓	$1,156,393
✓	✓	✓	$2,944,911
✓ (partial)	✓	✓	$5,151,335
	✓		$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
✓		✓*	$1,457,609
✓	✓	✓	$5,427,404
✓	✓	✓	$5,181,110
			$2,108,270
✓	✓	✓	$2,308,270
✓ (partial)		✓	$2,747,726
✓		✓	$2,108,270
✓ partial)	✓	✓	$2,951,780
	✓	✓*	$8,018,149
✓ (partial)			$2,108,270
✓	✓	✓	$5,204,181
✓		-	$1,858,270
✓ +	✓	✓	$5,798,571
	✓	✓ for EDL only	$3,138,319
✓	✓	✓*	$2,757,727
	✓	✓	$1,978,796
✓ (partial)	-		$2,108,270

Center for Immigration Studies

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 may 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/cbid/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://cft.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

962 Wayne Avenue, Suite 701
Silver Spring, MD 20910
(301) 563.6001
Fax: (301) 563.6012

NATIONAL ASSOCIATION FOR PUBLIC HEALTH STATISTICS AND INFORMATION SYSTEMS

Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards

Statement for the Public Record

by

National Association for Public Health Statistics and Information Systems

to the

Subcommittee on Crime, Terrorism, and Homeland Security

Committee on the Judiciary

United States House of Representatives

March 21, 2012

Mr. Chairman and Members of the Subcommittee—

The National Association for Public Health Statistics and Information Systems (NAPHSIS) welcomes the opportunity to update you on its activities to date in building the infrastructure necessary to support identification verification and discuss the ongoing challenges. NAPHSIS represents the 57 vital records jurisdictions that collect, process, and issue birth and death records in the United States and its territories, including the 50 states, New York City, District of Columbia and the five territories. NAPHSIS coordinates the activities of the vital records jurisdictions by developing standards, promoting consistent policies, working with federal partners, and providing technical assistance to the jurisdictions.

Vital Records Serve Important Civil Registration Function

Vital records are permanent legal records of life events, including live births, deaths, fetal deaths, marriages, and divorces. Their history in the United States dates back to the first American settlers in the mid-1600s, and in England as early as 1538.[1] More than 8 million vital events were recorded in the United State in 2009.[2]

Many organizations and millions of Americans use these records—or certified copies of them—for myriad legal, health, personal, and other purposes.

- Birth certificates provide proof of birth, age, parentage, birthplace, and citizenship, and are used extensively for employment purposes, school entrance, voter registration, and obtaining federal and state benefits (e.g., Social Security). Birth certificates are the cornerstone for proving identity, and as breeder documents are thus used to obtain other official identification documents, such as driver licenses, Social Security cards, and passports.

- Death certificates provide proof of date of death, date and place of internment, cause and manner of death, and are used to obtain insurance benefits and cease direct benefit payments, transfer property, and generally settle estates.

The federal government does not maintain a national database that contains all of this information. Consistent with the constitutional framework set forth by our founding fathers in 1785, states were assigned certain powers. The 57 vital records jurisdictions, not the federal government, have legal authority for the registration of these records,

[1] *U.S. Vital Statistics System: Major Activities and Developments, 1950 – 1995.* Centers for Disease Control and Prevention, National Center for Health Statistics. Feb 1997. Available online at: http://www.cdc.gov/nchs/data/misc/usvss.pdf

[2] National Center for Health Statistics, Centers for Disease Control and Prevention. Available online at http://www.cdc.gov/nchs/data/databriefs/db16.htm and http://www.cdc.gov/nchs/data/nvsr/nvsr58/nvsr58_25.pdf

which are thus governed under state laws. The laws governing what information may be shared, with whom, and under what circumstances varies by jurisdiction. In most jurisdictions, access to records is restricted to family members for personal or property rights, to government agencies in pursuit of their official duties, or for research purposes. In other jurisdictions, release of records may be subject to less restrictive limitations; and in a few states identifiable information from records is publicly available.

Because birth certificates are essential legal documents linked to identity, and because criminals need new identities to carry out their crimes, birth certificates are sought out and used to commit fraud, identity theft, and even terrorist activities. Studies have shown there are generally two types of vital records fraud: (1) when a fraudulent vital record is used by an individual; and (2) when a legitimate vital record is used by an imposter.

There are more than 14,000 different versions of birth certificates in circulation, issued by more than 6,400 state and local vital records jurisdictions. The sheer number of different versions of birth certificates makes it nearly impossible for anyone to manually differentiate a valid birth certificate from a counterfeit. The result is that criminals can and do easily assume new identities to commit crimes. It is therefore essential that birth and death records be secured and protected, and that federal and state agencies have the ability to verify the source data contained therein.

The Need for Identity Verification

Prior to the terrorist attacks on the United States on September 11, 2001, all but one of the terrorist hijackers acquired some form of identification document, some by fraud, and used these forms of identification to assist them in boarding commercial flights, renting cars, and other necessary activities leading up to the attacks. In its final report, The 9/11 Commission recommended implementing more secure sources of identification, stating the "federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."[3]

There are other cases where individuals have obtained birth certificates of deceased persons and assumed their identity, created fraudulent birth certificates, and altered the information on a birth certificate, as documented in a Department of Health and Human Services Office of Inspector General Report of 2000.[4] In 2009 and 2010, the Government Accountability Office (GAO) documented several cases in which investigators created fraudulent birth certificates and were able to obtain passports based upon the fraudulent

[3] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States, July 2004, p. 390.
[4] Department of Health and Human Services, Office of Inspector General, *Birth Certificate Fraud*, Sept. 2009 (OEI-07-99-00570).

records because the passport office did not verify the birth certificate information.[5] In 2011, the Federal Bureau of Investigation arrested Khalid Ali-M Aldawsari for "attempted use of a weapon of mass destruction." When the FBI searched Aldawsari's apartment, agents discovered that Aldawsari had plans to obtain a forged U.S. birth certificate and obtain multiple drivers' licenses for the purpose of renting several different cars to carry out his attacks. Aldawsari recognized that birth certificates can be used to obtain multiple identification documents such as passports and driver's licenses.

EVVE is an Effective Tool in Preventing Fraud, Identity Theft, and Terrorism

Heeding the recommendations of the 9/11 Commission, Congress enacted the REAL ID Act in May 2005. The REAL ID Act and its corresponding regulations (6 CFR Part 37) require that applicants for a driver's license present their birth certificate to the motor vehicle agency to validate their U.S. citizenship and their date of birth, and that birth certificates must be verified by the state. Sec. 37.13 of the identification standards regulations recommends that states through their departments of motor vehicles (DMV) should use the Electronic Verification of Vital Events (EVVE) system, operated by NAPHSIS, to verify birth certificates presented by applicants.

EVVE is an online, query-based system that verifies birth certificate information. It provides authorized users at participating agencies with a single interface to quickly, reliably, and securely validate birth and death information at any jurisdiction in the country. In so doing, *no personal information is divulged* to the person verifying information—EVVE simply relays a message that there was or was not a match with the birth and death records maintained by the state, city, or territory.

With support from the Department of Homeland Security (DHS), NAPHSIS has now installed EVVE in 38 vital records jurisdictions, with 10 jurisdictions in the process of implementation. NAPHSIS has also procured a data analysis and quality control tool that all jurisdictions can utilize to analyze their EVVE data for anomalies, inconsistencies, accuracy, and completeness. This tool and the analysis of EVVE data has been completed in 30 jurisdictions to-date.

EVVE is currently used by several federal and state agencies to verify identification and authenticity of birth certificates.

- As part of a seven-year pilot program funded by the DHS, three state DMVs—North Dakota, South Dakota, and Iowa—used EVVE to validate U.S. citizenship and date of birth, and verify the authenticity of birth certificates presented to obtain drivers' licenses. As of 2011, the pilot funding is no longer available and these DMVs have thus discontinued their use of EVVE to verify identity on state-issued drivers' licenses.

[5] Government Accountability Office, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, Mar. 2009 (GAO-09-447) and *State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud*, July 2010 (GAO-10-922T)

- The Department of State's Passport Fraud Prevention Managers commenced using the EVVE system in March 2009 for birth certificate verifications. In their first six weeks of use, there were two instances where the Fraud Prevention Mangers used the EVVE system to electronically verify the birth certificates, and EVVE returned a 'no match.' Upon further follow up with the vital records offices that 'issued' the birth certificates it was determined that indeed the birth certificates presented with those passport applications were fraudulent. Based on these and other successes, NAPHSIS is currently working with the Department of State Passport Services to improve usage volume of EVVE.

- The Social Security Administration, which funded the initial development and testing of EVVE in 2001, uses the system to verify proof of age and place of birth as a program policy requirement.

- The Deficit Reduction Act of 2005 requires the verification of citizenship and identity for enrollment in Medicaid through a birth certificate or other official document. The South Dakota Medicaid Office was the first to use EVVE for this purpose in 2007, followed by Medicaid Offices in Mississippi, Minnesota, and Washington. Since then, several other states have inquired about using EVVE.

These EVVE users—as well as voluntary users at the Office of Personnel Management, the Army National Guard, and other state agencies—are enthusiastic about the system, citing its usability and ability to protect against fraudulent activities, safeguard the confidentiality of data, and improve customer service.

Federal Investment in Infrastructure Could Help Speed EVVE Adoption

Despite EVVE's security, speed, and ease of use, the system is only as good as the underlying data infrastructure upon which it relies. EVVE faces resource-related challenges that may impact our ability to harness the system's full potential:

- Most vital records jurisdictions have electronic birth records that extend back for several decades, and the utilization of the EVVE system has proven that these databases can be used effectively. However, only 85 percent of birth records dating back to 1945 are available in electronic form. To recognize EVVE's full potential to protect our nation, 100 percent of birth certificates in 100 percent of jurisdictions should be in electronic form. In addition, some data should be re-keyed to improve quality. Among the vital records jurisdictions that participated in the American Association of Motor Vehicle Administrators (AAMVA) birth verification pilot, those jurisdictions that have not cleaned up their files are experiencing only a 90 percent match rate. With clean data files, the match rates would exceed 95 percent.

- There are cases where an individual has assumed a false identity by obtaining a birth certificate of a person who has died. Therefore, it is important that resources be provided so that all death records are electronically linked to birth records. Most

jurisdictions have linked infant deaths, and in many cases linked deaths to persons under 45 years of age. In the cases where birth and death records are linked, EVVE will return a "deceased" indicator to the requesting agency, which will confirm that the documentation presented is fraudulent.

- NAPHSIS collects fees from EVVE users to cover costs related to the system's operation, such as technical support and maintenance, system and business operation support, and vital records jurisdiction fees to support EVVE query access to birth data. Providing federal funding to DMVs to cover these costs could increase EVVE usage and help prevent the fraudulent use of birth information in acquiring driver's licenses and identification cards. Since the transaction fees are volume based, the more EVVE users, the lower the costs of use will be.

The jurisdictions' efforts to digitize, clean, and link vital records have been hindered by state budget shortfalls. In short, the jurisdictions need the federal government's help to complete building a secure data infrastructure in support of electronic identity verification.

DHS is in the earliest stages of supporting a new project to close loopholes that contribute to identity fraud. In this "reciprocal pilot," three DMVs will use the EVVE system to verify birth certificates, and three vital records jurisdictions will use the DMVs' driver's license verification system to verify driver's licenses that individuals present to obtain copies of birth certificates. The development of the interface should take about one year and once installed, the pilot will last 14 months. During the pilot, the DMVs and vital records jurisdictions will jointly investigate instances of "no matches," determining why a no match occurs and developing business practices to handle no matches.

The 9/11 terrorists' ability to obtain valid government issued IDs, and the GAO's ability to obtain passports using fraudulent birth certificate data, reinforces the merits and importance of the birth verification. We feel strongly that investment in EVVE will strengthen Americans' safety and security by accurately, efficiently, and securely verifying birth data on the 245 million driver's licenses issued annually. More than one decade after our nation's darkest day, isn't it time to implement the 9/11 Commission's recommendations and secure official forms of identification?

NAPHSIS appreciates the opportunity to submit this statement for the record and looks forward to working with the Subcommittee. If you have questions about this statement, please do not hesitate to contact NAPHSIS Executive Director, Patricia W. Potrzebowski, Ph.D., at ppotrzebowski@naphsis.org or (301) 563-6001. You may also contact our Washington representative, Emily Holubowich, at eholubowich@dc-crd.com or (202) 484-1100.

IDENTITY DOCUMENTS

CALL TO ACTION: THE GROWING EPIDEMIC OF COUNTERFEIT IDENTITY DOCUMENTS AND PRACTICAL STEPS TO COMBAT IT

The commercial, academic and government members of the Document Security Alliance have teamed together to provide an informative summary of the growing epidemic of counterfeit identity documents and the practical steps to combat it. We stand prepared to provide assistance and answer questions to help government organizations improve the security of their identity documents.

CONTENTS

The Problem 1
DLs as Counterfeiting Targets ...2
Counterfeit IDs Impact 2
Enforcement Overwhelmed 2
Solutions to the Epidemic 3
What Can Congress do to Help ...4
What Laws are Used 4
DSA Recommendation 4
Appendix 5

December 2011

THE PROBLEM – HIGH QUALITY COUNTERFEITS ARE FLOODING AMERICA

Off-shore counterfeiting rings in particular, and counterfeit rings resident in the United States are using scanning and image manipulation technology along with advanced software and printers to produce counterfeit driver's licenses which are very difficult to discern from valid driver's licenses. These counterfeits are being successfully passed in a variety of critical day-to-day situations.

Because of REAL ID Act compliance and increased use by states of identity verification systems such as SSOLV and SAVE, those living or operating under assumed names are increasingly finding themselves blocked at driver's license issuing agencies when attempting to get "valid" identification. Consequently, they seek high quality driver's license counterfeits and counterfeit "breeder documents" such as birth certificates.

There is a growing sophistication in high quality counterfeit driver's licenses and state issued IDs, some of which are produced overseas and others in major metropolitan areas by professional criminals. In particular, there is a virtual flood of low cost, high quality counterfeits being shipped by the tens of thousands from China via the website *IDChief.ph*. Although this site is the most prominent, it is not unique.

Enforcement of important U.S. laws, as well as our safety and security is threatened, as purchasers of counterfeit IDs use them for purposes beyond underage drinking. The federal program for verifying eligible employees (E-Verify) and the National Instant Criminal Background Check System (NICS) used by gun stores to comply with the Brady Handgun Violence Protection Act both depend on the reliability of IDs (usually driver's licenses) presented by those subject to the check.

Federal and state laws recognize three types of "false" identity documents:

1. Counterfeit identity documents that emulate the features and characteristics of valid IDs issued by state and federal governments. For decades, the preferred counterfeit ID is a counterfeit driver's license with an unexpired date.
2. Valid identity documents, usually issued in the name of a fictitious or stolen identity, obtained through fraudulent means.
3. Valid identity documents that have been altered after issuance to change a name, photo image, age, or other biographic descriptor.

IDENTITY DOCUMENTS

Driver's Licenses are a Favorite Target for ID Counterfeiters

Driver's licenses are the document of choice for identity purposes in the United States.

- A valid driver's license will get someone onto any domestic airline flight within the United States.
- Visual authentication of any secure document, such as a driver's license, normally requires the inspector to make a quick determination that features from the document, like the photograph, demographic information, security features, and substrate are genuine.
- Driver's licenses or passports are required for Brady Gun Checks and by employers using E-Verify. They are also required as proof of identification for boarding airplanes and for listed (controlled) pharmaceutical products like Oxycontin and Methamphetamine.

Counterfeit IDs Impact National Security, Homeland Security, Public Safety and the Economy!

Public Safety: (1) Underage drinking and habitual DUI offenders on the highways; (2) Increased levels of fraudulent retail and internet purchases of controlled substances such as amphetamines, barbiturates, and narcotics such as hydrocodone and oxycodone.

According to the Department of Justice, in 2007, American society suffered an estimated $193 billion in losses from illicit drug use through crime, health and productivity costs. A 2011 report indicated that 16% of inmates in federal prisons convicted on forgery and fraud charges have their offenses classified as "drug-induced". Additionally, 39% of those in jail and 42% of those in state and local prisons on convictions of forgery and fraud have their crimes classified as "drug-induced".[1] In nearly all cases, the link occurs because drug addicts can purchase controlled drugs using counterfeit IDs, especially when combined with counterfeit doctors' prescriptions.

Homeland Security: Increased levels of illegal gun purchases as brought to light by recent Mexican cartel activities and drug distribution rings in major U.S. cities. Using a counterfeit driver's license is a common method used by felons and straw purchasers to avoid detection by NICS checks.

Over the last five years, Mexican authorities have confiscated over 94,000 firearms, 64,000 of which originated in the US. Weapons from "Fast & Furious", are coming back into the US.[2] It has been known for many years felons and straw buyers of guns rely on fake IDs to disguise their true identities, so many arrested are convicted of forgery and fraud as well as for illegal gun purchases.[3]

National Security: Jihadist terrorists and homegrown extremists have used counterfeit driver's licenses to rent cars and trucks, and to buy chemicals or certain fertilizers to derive high potency explosive components. Examples include Oklahoma City bomber Timothy McVeigh.

The 9/11 Commission Report states unequivocally that "Travel documents are as important as weapons" (p. 384) Recently, the indictment of terrorist suspect Ali Saleh Kahlah al-Marri, who has been linked to alleged Sept. 11 paymaster Mustafa Ahmed al-Hawsawi, stated that al-Marri was arrested with a laptop computer that had 1,000 stolen credit cards account numbers on it, along with a host of Internet bookmarks pointing to fraud and fake ID-related sites.

Crime: The "DC Sniper" John Muhammad was a proficient dealer in counterfeit driver's licenses, both to assist his illegal alien smuggling activities in Antigua, and for domestic criminal purposes.

Criminals often use counterfeits to conceal their fictitious or stolen identities to commit crimes, and/or hide from law enforcement.

The Ben Bernanke check fraud case was part of a multi-state gang operation that successfully used counterfeit driver's licenses to drain bank accounts.

State and Federal Law Enforcement Are On the Job but Overwhelmed

Enforcing federal laws is critical to stopping the flood of counterfeit driver's licenses. To constrain lawbreakers using counterfeit IDs, an ounce of prevention, through an aggressive defense, will enhance public safety and significantly reduce financial losses to federal agencies and institutions. The resources expended to prosecute the providers and users of counterfeit ID's are a fraction of the benefit returned in reducing economic losses experienced by both the federal government and commercial businesses.

---

[1] Department of Justice: National Intelligence Center. "Economic Impact of Illicit Drug Use on American Society." April 2011. Pp ix, 58-62.

[2] "[O]f the nearly 94,000 [weapons] that have been recovered that have been traced in Mexico in recent years, over 64,000 of those guns were sourced to the United States of America; 64,000 of 94,000 guns sourced to this country."- Attorney General Holder, 11/8/11, Senate Judiciary Committee Hearing.

[3] Pierre Thomas, "In the Line of Fire: The 'Straw Purchase' Scam," The Washington Post (August 14, 1991); and Thomas, "Va. Driver's Licenses Loophole for Guns; Fake Addresses Used in No-Wait Sales," The Washington Post (January 20, 1992).

IDENTITY DOCUMENTS

This summer (2011), U.S. Custom and Border Protection spokesman Brian Bell described the surge of counterfeit IDs coming in from overseas. "Since January we have caught about 15,000 IDs," Bell said. "In the past we would see maybe 10 to 15 per year." In July 2011, officers in a Chicago suburb arrested 40 students between the ages of 17-20 for licenses that were hidden inside a game shipped from China. The shipment contained 1,700 fake IDs, according to the Cook County Sheriff's office.[8]

In February, a high-tech fake identification mill in Layton, Utah was dismantled by the Utah Attorney General's SECURE Strike Force when special agents arrested three illegal aliens and seized equipment used to make a wide assortment of identity cards from different states and countries. Agents seized computers, printers, laminating machine, cutters and high quality blank printing stock. They also confiscated Mexican consular identification cards, driver licenses from Utah and other states, Social Security cards and electrician licenses. SECURE Strike Force Commander Rhett McQuiston said, "We found incredibly realistic-looking identification documents. We have also never seen anyone creating false identification cards from so many states and federal government agencies."[9]

Also in February, investigators from the North Carolina Motor Vehicle Department responded to a tip from a temporary agency that people were using what appeared to be fake identification documents when applying for jobs. Investigators found fake driver's licenses from several states including North Carolina, Texas and California. They also found fake Social Security Cards and Permanent Resident cards. "They had the capability of making fake ID's from any state," lead investigator Jessica Walker said. Although the suspects in this case are illegal Mexican immigrants, that's not always the case, said District Supervisor Rena Rikard of the Department of Motor Vehicles. "There are a lot of people out there doing this," she said. "It's not just Mexicans who are doing it either – it's everybody."

The recent wave of foreign produced high quality Fake IDs are difficult to discern without the use of technology or people well trained in forensic document analysis, using the special tools of the trade. Those states working to comply with REAL ID rules are training DMV personnel and local law enforcement to recognize counterfeit Driver's Licenses, notably Ohio, New Jersey, New York, Connecticut and Florida. Many other states, however, provide little or no comparable forensic document training to local law enforcement. There is also very limited use of card scanning technology by state and federal law enforcement or security personnel at ID checkpoints at airports and elsewhere.

There are Solutions

Law enforcement actions by federal officials, led by the FBI and ICE, are notable, but are only capable of arresting a small proportion of the criminal gangs who produce and sell the counterfeits. To be more effective, the following solutions should be considered:

Train our gatekeepers: Frontline personnel in vulnerable areas of commerce, federal building security personnel and local police should become trained in basic methods of identity document authentication, and have tools available to assist in distinguishing counterfeit IDs from valid IDs. Reference guides to state licenses are essential tools for authentication, as counterfeit driver's licenses are most often used in states other than the state from which the document is counterfeited.

Stronger card security for state and federal issued IDs and Driver's Licenses:

- Incorporation of levels 1, 2, and 3 security features into documents.
- Better understanding and usage of advanced authentication technologies. There are a variety of effective, easy to verify optical technologies which cannot be easily copied. These can be combined with other level 2 and 3 security features to form a layered approach to security that has proven effective.

Specialized and secure card production materials designed to prevent counterfeiting and that are limited in access and costly to obtain.

Use of ID card scanning technology for routine inspections of IDs to detect counterfeits

- Use of technology that does more than verify a bar code. Because sophisticated ID counterfeits produce bar codes that are impossible to differentiate from valid IDs, ID readers MUST be able to verify security features as well as bar codes.

---

[8] Slaver, Anna. Kent Page. "Kent State Students Reach Pleas on Fake ID Charges". 10/6/11.
[9] http://attorneygeneral.utah.gov/PR_0303110.html

IDENTITY DOCUMENTS

Congress Needs to Affirm our National Commitment to Reduce Financial and Social Losses from Counterfeiting

We recommend Congress emphasize strong support for enforcement of federal anti-counterfeit, law enforcement task forces. Congressional oversight should challenge the Office of U.S. Attorneys to actively prosecute alleged criminal offenders.

- Previously, ICE put more resources into counterfeit and fraudulent document task forces. This has been de-emphasized over the past two years. Congressional interest in DHS' efforts to investigate and prosecute criminal rings would increase ICE's resource allocation. The FBI has begun to more actively investigate and prosecute international criminals using counterfeit identity documents. Congressional support for these activities would lead to a greater resource allocation by the Department of Justice.

We recommend the continuation of Department of Homeland Security grants supporting forensic document training for local law enforcement.

- These grants expand the capability of state and local police to identify those presenting counterfeit documents. This is of great importance as those representing local governments are the first lines of defense against counterfeit identity documents.

We recommend Congressional committees of jurisdiction request a GAO review of the federal agencies involved in fraud and counterfeit defense to assess and measure their improvements. They should consider adding this requirement to the respective Offices of Inspector General of the federal agencies most at risk of financial loss through crimes enabled by counterfeit identity documents.

- Existing federal laws to penalize the use of counterfeit IDs are tangential to other fraud statutes – hence these crimes are rarely prosecuted. Additional Congressional Oversight would increase attention to requiring use of federal agencies to identify counterfeit IDs used to access federal buildings.

Law enforcement agencies can use existing federal laws to prosecute and penalize criminals who counterfeit IDs and driver's licenses!

1. 18 U.S.C. Section 1028(a)(5) B Possession of Document-Making Implements;
2. 18 U.S.C. Section 1028(a)(8) B Trafficking in False Authentication Features;
3. 18 U.S.C. Section 1342 B Using a Fictitious Name or Address;
4. 18 U.S.C. Section 1546 B Fraud & Misuse of Visas, Permits, & Other Documents;
5. 18 U.S.C. Section 371 B Conspiracy;
6. 18 U.S.C. Section 1326(a), (b)(2) B Illegal Alien Found in the U.S. Following Deportation

A 2011 Los Angeles criminal case illustrates how federal statutes were used to prosecute more than two dozen individuals in a massive fraudulent document operation. The ID ring was producing counterfeit driver's licenses for 40 of 50 U.S. states. These counterfeit IDs were used in the "commission of credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion schemes... the false document manufacturing ring produced raw materials for the manufacture of thousands of documents per month that were distributed in California and across the United States."[40]

The DSA recommends our Congressional leadership support counterfeit ID prevention in a manner that prioritizes public safety, fraud reduction, and the optimization of collected revenues.

ID counterfeiting facilitates a wide range of illegal activities. The cost to society far exceeds the naïve popular perception that "Fake IDs" are only for underage kids trying to get into a tavern. Counterfeit IDs are a primary means to fraudulently obtain access, benefits, and prescription drugs for illegal use. Transnational criminal gangs operate across the United States counterfeiting driver's licenses, birth certificates, and other Identity documents costing consumers, businesses and government benefits agencies hundreds of $millions annually. ID Counterfeiting has become a major gateway for criminals to steal, injure and, in some cases, terrorize the public.

Federal laws sufficient to criminalize ID counterfeiting already exist, as do the agencies authorized to enforce them. As Congress considers how best to reduce the current deficit, it's important to consider that the fraud prevention savings to commerce and society well exceeds enforcement costs. Our nation's commitment to continue to fund identity document protection should not be in question

[40] FBI Press Release 11/3/11: http://www.fbi.gov/losangeles/press-releases/2011/more-than-two-dozen-charged-in-massive-fraudulent-document-counterfeiting-conspiracy-in-southern-california-involving-manufacturing-transportation-selling-distribution-and-sale-of-counterfeit-identity-documents#ixzz1dSIU

IDENTITY DOCUMENTS

APPENDIX

Important Federal Definitions to Prosecution of ID Counterfeiting Crimes:

TERM	DEFINITION	US CODE
Authentication Feature	the term "authentication feature" means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;	18 USC 1028 (d)(1)
Identification Document	the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;	18 USC 1028 (d)(3)
False Identification Document	the term "false identification document" means a document of a type intended or commonly accepted for the purposes of identification of individuals that-- (A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and (B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization	18 USC 1028 (d)(4)
False Authentication Feature	the term "false authentication feature" means an authentication feature that-- (A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit; (B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or (C) appears to be genuine, but is not	18 USC 1028 (d)(5)
Issuing Authority	the term "issuing authority"-- (A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and (B) includes the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization	18 USC 1028 (d)(6)

204 E Street, NE
Washington, DC 20002
Phone: 202/543-5552
Fax: 202/547-6348
www.documentsecurityalliance.org
info@documentsecurityalliance.org

DSA
DOCUMENT SECURITY ALLIANCE

The Document Security Alliance (DSA) is a not-for-profit organization created by government agencies, private industry and academia in the months after September 11, 2001. Since that time DSA has worked to improve document security at all levels of government and enhance our nation's economic, personal, and homeland security for the 21st century. DSA's goal is to identify methods of improving security documents and related procedures to combat fraud, terrorism, illegal immigration, identity theft, and other criminal acts. The DSA members - in both government and private industry – draw upon a wide range of knowledge and detailed technical disciplines to accomplish this goal. The group is committed to developing recommendations for appropriate federal and state government agencies, private industry, and policymakers

IDENTITY DOCUMENTS

ATTACHMENT 1: FRAUDULENT DOCUMENT ENTERPRISE

THIRTY INDICTED IN US COURT FOR INVOLVEMENT IN VIOLENT IDENTITY DOCUMENT COUNTERFEIT RING

A Flourishing Fraudulent Document Enterprise (FDE):

This particular Fraudulent Document Enterprise (FDE) [1] was a massive, complex, and transnational counterfeit identification document manufacturing ring, operating in 19 different U.S. cities across 11 states, with a base of operations in Mexico. The criminal organization's members and associates engaged in the illegal acts of false document trafficking, money laundering, kidnapping and murder. FDE is a highly organized gang with a cell based structure, a multi-level chain of command, and supervision from within Mexico. Federal prosecutors say the organization functioned like a "multinational corporation". The group was identified and "dismantled" by Immigrations and Customs Enforcement (ICE) agents, charging thirty for their involvement within the enterprise. Twenty seven of the defendants have pleaded guilty. However, the management team remains at large in Mexico, and it is likely that new FDEs will be established to meet the demand.

ICE reports that this gang was unique only for its high level of violence, but similar counterfeit document rings are operating all over the country. The gang's leader went by the name "El Muerto," Spanish for the "dead one." The gang did not hesitate to attack competing gangs with physical force or murder.

Counterfeit IDs Manufactured and Sold:

This gang produced and sold driver's licenses, state ID cards, foreign driver's licenses, Permanent Resident Alien cards, Social Security cards, foreign identification cards. Nearly 2,000 fraudulent documents were seized by authorities, along with computers, printers, packages of card-making stock, and other miscellaneous document making tools.

Where:

Virginia Beach, VA
Chelsea, MA,
Richmond, VA,
Norfolk, VA ,
Manassas, VA
Fayetteville, AR
Little Rock, AR
New Haven, CT
Mishawaka, IN
Lexington, KY
Louisville, KY
St. Louis, MO
Chapel Hill, NC
Greensboro, NC
Raleigh, NC
Wilmington, NC
Cincinnati, OH
Providence, RI
Nashville, TN

[1] A Fraudulent Document Enterprise is defined by Title 18, USC, Section 1961(4) that is a group of individuals associated in fact although not a legal entity. An FDE is a form of organized crime. In this particular case, the gang was also part of a transnational organized criminal gang, where the owners and managers are located outside the United States.

DSA
DOCUMENT SECURITY ALLIA

Murder:

Gang cells used strong violence to drive out competition within each city of operations, including kidnappings, beatings, and murder. In July 2010, Edy Oliverez-Jiminez, the leader of the gang's Little Rock cell, kidnapped a competitor, bound, gagged, and blindfolded him and then beat him to death.

Money:

The documents were sold at $150 - $250 per set of two. Usually, this was a Permanent Resident Alien (Green) card along with a Social Security card, for example. A tracking of Western Union wire transfers from cell leaders to upper management in Mexico showed a total of more than $1,000,000 in illicit funds moved from January 2008 to November 2010.

Can the Widespread ID Counterfeiting Enterprises Be Stymied by Prevention?

Too many state drivers' licenses are too easily counterfeited. Because driver's licenses will only become more valuable to felons and others as a way to evade federal and state laws in the future, it's critical that state DMVs incorporate new technologies in identity documents issued, including driver's licenses. Many of these new technologies have proven to be nearly counterfeit proof. Had the targeted states' driver's license issuing agencies incorporated more security features into their documents, the driver's licenses and ID cards would not have "passed" scrutiny and been so widely accepted. States can also do much more to provide training to merchants, banks, and employers so they are alert to counterfeit IDs.

Quotes:

The gang is "devoted to the production and sale of false identification documents".

- Federal Indictment

They really ran this like a business and used a business model where people would be promoted based on the amount of money they brought in.

- John Torres, ICE

Based on the guilty plea today, the hope and expectation is that it will have a chilling effect ... on this type of activity.

- Neil MacBride, Federal Prosecutor overseeing the case

Far-reaching fake document ring

Sources:

United States District Court for the Eastern District of Virginia v. Israel Cruz Milan, et al. Criminal No. 3:10cr308. 2/23/11.

O'Dell, Larry. "U.S. fake ID case nets guilty plea". Associated Press. 11/16/11.

Johnson, Kevin. "Prosecutors pursue fraud ring, cite 'unprecedented' violence". USA Today. 3/7/11

"Guilty plea for man in violent fake ID case". Associated Press. 11/15/11.

December 2011

IDENTITY DOCUMENTS

ATTACHMENT 2: WHERE DRIVER'S LICENSES AND ID CARDS ARE REQUIRED PROOFS OF IDENTITY

WHERE ARE DRIVER'S LICENSES REQUIRED AS PROOFS OF IDENTITY?

A driver's license is the preferred identification document for law enforcement, employment and commercial businesses. It is only when a patrolman stops a speeding driver, or a traffic accident occurs, that a driver's license is used to prove lawful eligibility to operate a motor vehicle. When we stop at a bank teller line, or the bank's drive through teller, we are accustomed to provide our driver's license as proof of identity to cash checks or withdraw funds. A driver's license is used to prove identity to apply for a job, purchase a gun, or board an airplane. Every adult needs a driver's license or a state issued identification card as a fact of everyday life.

As security measures have tightened throughout the past decade, so has the need for accurate identification verification. Along with airports and federal facilities, businesses have also been increasingly reliant on the driver's license as an accurate proof of identity.

The listed locations require driver's licenses and state issued ID cards or passports. That is, everyone must offer proof that you are who you say you are.

The locations are categorized as National Security, Homeland Security, and Public Safety, as well as all three combined.

National Security
Maritime workers
Ports

Homeland Security
Federal facilities
Cruise ships
Truck rental office

Public Safety
Teachers
Home health care workers
Elder care workers
Child care providers
Indian gaming
Nursing homes
Loan originators
SSA offices
Public assistance offices
Tavern
Restaurant
Check cashing offices
Banks
Credit unions
Office of vital records
Post office
Courthouses
Hotels
Sporting goods stores
Retail alcohol / tobacco sales locations
Public schools
Colleges
Casinos
Pharmacies
Voting/registration polling places
Jury duty
Town clerk
Marriage license

All of the Above
Private security guards
Airport workers
Hazmat drivers
TSA
DMV
Firearms dealers
Employers
Highway patrol
Trains
Office building security

204 E Street, NE
Washington, DC 20002
Phone: 202/543-5552
Fax: 202/547-6348
www.documentsecurityalliance.org
info@documentsecurityalliance.org

DSA
DOCUMENT SECURITY ALLIANCE

Prepared Testimony for Brian Zimmer
President, Coalition for a Secure Driver's License

U.S. House of Representatives Committee on the Judiciary
Subcommittee on Terrorism, Technology and Homeland Security
On
"Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards"

Washington, DC
March 21, 2012

The Coalition for a Secure Driver's (CSDL) is pleased to have the opportunity to provide the Subcommittee with comments for the record in connection with the Subcommittee's hearing entitled, "Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards."

CSDL would like to thank Subcommittee Chairman F. James Sensenbrenner and Judiciary Committee Chairman Lamar Smith for their leadership and for holding this hearing. Since the REAL ID Act's enactment, Congressman Sensenbrenner and Chairman Smith have been true champions of the states. They have supported state funding for compliance with the REAL ID's regulatory standards and ensured that the Department of Homeland Security (DHS) fulfills its mission to assist the states move towards securing the driver's license adjudication and issuance processes. Letters and statements authored by Representatives Sensenbrenner and Smith regarding the REAL ID Act serve as strong examples that Congress has not forgotten the lessons learned from the September 11, 2001 attacks.

Leading up to the attacks, eighteen of the nineteen September 11th hijackers obtained a total of more than thirty (30) state driver's licenses and ID cards from states including; Florida, Virginia, California and New Jersey. These IDs allowed the terrorists to move freely throughout the Eastern United States and facilitated their boarding of commercial airliners which they used as weapons against American citizens. In 2004, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recommended that, "[T]he federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses."

The REAL ID Act established these standards by statute. Title II of the REAL ID Act directed DHS to establish minimum security standards for state motor vehicle agencies. The Act was quite specific and proscriptive, because Congressional analysis had identified the areas in which the states' rules were absent or weak with regard to preventing imposters, including foreign terrorists, from exploiting those vulnerabilities. In 2008, detailed regulations were issued setting standards and benchmarks for issuing driver's licenses. The law is binding only on the

Coalition for a Secure Driver's License 1300 Pennsylvania Avenue NW, Suite 880, Washington D.C. 20004
Tel: (202) 312-1540

federal government. However, states that issue driver's licenses and IDs which do not meet REAL ID's regulatory standards cannot be accepted by federal agencies after certain deadlines. Last year, the date on which the federal government can no longer accept for identification purposes driver's licenses from non-compliant states was extended by Secretary of Homeland Security Janet Napolitano to January 15, 2013.

All states remain free to issue and to accept non-compliant IDs for state purposes, so long as they clearly marked "not for federal identification purposes."

That's an important distinction because if the state has not held all applicants to the REAL ID standard, there needs to be a "buyer beware" warning on the lower class of IDs. It is important to distinguish unreliable identity documents issued by the states or other credential issuing agencies from those that accurately and completely establish the bearer's true identity. In an age of wide spread counterfeiting and fraud, this differentiation should be obvious to everyone, but unfortunately opposition to the REAL ID rules demonstrates it is not.

It is especially important that the Department of Homeland Security continue to make that distinction in its rules and regulations, in order to protect the nation's transportation systems from terrorists and transnational criminal organizations.

The Coalition for a Secure Driver's License strongly concurs with the Bipartisan Policy Center's position on the deadline extension. In 2011, the Bipartisan Policy Center issued its Tenth Anniversary Report Card on the status of the 9/11 Commission's recommendations. The report stated that "the deadlines for compliance have been pushed back twice to May 2011, and a recent announcement pushed back compliance again until January 2013. The delay in compliance creates vulnerabilities and makes us less safe. No further delay should be authorized; rather, compliance should be accelerated."

The authorities placed with the Department of Homeland Security by PL 109-13 (REAL ID Act) regarding the states' issuance of driver's licenses are permanent and continuous. The Act established deadlines for state compliance with federal rules pertaining to confirming identity of applicants prior to issuance of driver's licenses and state IDs. Because there is no national ID, and little interest in establishing a national ID, driver's licenses and state issued IDs are the default alternative. Hence, improving the reliability of these documents remains a priority for the federal government for purposes of homeland security, national security, and fraud prevention. Enforcement of REAL ID deadlines pertaining to public use of commercial airlines, access to public building have significant security implications and economic effects bearing on all levels of government and the private sector.

For law enforcement, most members of Congress, and the public, the issuance of secure identification documents including driver's licenses is important for highway safety, for

homeland security, and for national security. To this end, CSDL believes several steps could be taken to achieve full compliance by a substantial majority of the states.

Establish an Operational Program Office

The final rule promulgated by the Department of Homeland Security in 2008 specifically addresses the requirements for the states to report their compliance status every three years. However, there is no program office established within the department as a point of continuity and expertise for driver's license security and communication with the states.
REAL ID is a program involving all but the three or four states that opted out three years ago, involving hundreds of millions of dollars in grants, with a complex set of security requirements that require interstate and interagency coordination, and the Secretary has never established a program office to audit state motor vehicle agency compliance. Surely out of the billions of dollars under the DHS's discretionary control, a couple million can be found to manage this critical process.

The Congress has provided over $220 million in federal grants to the states to comply with REAL ID. These grants are supposed to be expended by the states to move toward compliance with REAL ID rules, yet the Department of Homeland has not established a program office to proactively guide the states with cost effective processes.

The lack of designated program office may have led to the Department's lack of responsiveness. Despite at least five states that have certified their compliance with REAL ID rules, those states have received no response from the Department. Those five states have demonstrated that REAL ID is doable in the short term and affordable, yet there is little or no communication by Homeland Security officials to other states about what needs to be done.

It is reported that none of the letters sent by the governors in response to the last deadline, since extended, have received a response from Secretary Napolitano. States still lack written guidance from the department, four years after the final rule. The Department of Homeland Security should not continue to keep the states waiting for direction.

Given the scale of the responsibilities and project schedule, there should be a minimum of five Full Time Employees, including a designated office director. The program office costs, including travel, can operate for less than $2 million per fiscal year, or about 1% of the federal grants already expended for REAL ID compliance. With a committed staff and a modest budget, DHS could begin to address directly its responsibilities with the compliant states, which currently number over twenty, with another twenty plus to follow. This a fraction of the number of personnel at the Department of Transportation devoted to the other driver's license related public safety programs.

Ideally, the REAL ID Program office would work closely with the Federal Motor Carrier Safety Administration (FMCSA). FMCSA already conducts audits of state Commercial Driver's License (CDL) issuance and a partnership between FMCSA and the REAL ID program office would allow concurrent audits of CDLs and REAL ID compliant driver's license rules.

The REAL ID program offices should be placed within the National Protection and Programs Directorate (NPPD), which contains DHS components who will be essential to the actual enforcement of the REAL ID rule. NPPD has a suitable governance culture because the agency components are comfortable working with state agencies and the private sector via persuasion versus regulatory authority. REAL ID authorities are tied to voluntary compliance by the states, which means the program office philosophy will align with "you should" versus "you must." NPPD is highly specialized and is managed by an Under Secretary. It contains within it most support functions needed by the REAL ID program office going forward. NPPD has demonstrated competence managing large programs. REAL ID rules incorporate the need to secure large systems and personal information from hacking. This correlates well with the NPPD's Office of Cybersecurity and Communications, as well as the Office of Infrastructure Protection. NPPD is also a logical agency component for the REAL ID enforcement for access to nuclear plants.

The goal of the National Protection and Programs Directorate is "to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements." Similarly, REAL ID is a key component of the secure identification layer of homeland security.

Coordination with the Federal Protective Service and the Transportation Security Administration on procedures and policies for the deadline of federal enforcement

The Federal Protective Service would be one of the enforcement arms for the REAL ID mandate that access to federal buildings will eventually be restricted only to REAL ID compliant driver's licenses and IDs. Clearly, the most important enforcement agency is the Transportation Security Administration.

The recommended REAL ID Program Office could assist with a coordinative outreach to the states, ensuring continuity of enforcement at federal facilities, airports, and nuclear power plants with the Federal Protective Service and the Transportation Security Administration. There are fifty-six (56) jurisdictions that issue driver's licenses and identification cards, so an active and effective communication link needs to be established. The Program Office should establish a plan to differentiate states that issue compliant driver's licenses and IDs. Transportation Security and Federal Protective Service personnel will need to be trained to recognize these IDs and take secondary inspection measures to holders of non-REAL ID compliant driver's licenses. This would send a strong signal to states that choose not to comply or have not made substantial progress that the deadline is eminent. Noncompliant states could

then give their residents ample notice to obtain alternative documentation such as a U.S. Passport.

Leverage New Technology at Airports to Facilitate Faster Inspection

The Transportation Security Administration (TSA) may be able to leverage the Credential Authentication Technology/Boarding Pass Scanning System (CAT-BPSS) machines that are currently being tested at twenty (20) airports across the country. These machines enable the Transportation Security Administration officers to electronically identify fraudulent identification documents and boarding passes. TSA and the Department should use this pilot phase to include software that distinguishes between compliant and noncompliant driver's licenses. As new states begin issuing compliant driver's licenses, the software should be flexible to incorporate these upgrades.

Conclusion

Compliance with the REAL ID driver's license security standards will finally lead to realizing the goal of "one driver, one license". This is the logical extension of the highly successful "one driver, one license" for commercial truck drivers that has improved safety on our highways. REAL ID promotes safety by denying people who have lost their driver's license in one state from simply assuming another identity in another state to get a new driver's license. These people are shopping for a new identity because of reckless driving or driving while intoxicated, or for vehicular manslaughter, and it's important to stop them before they kill someone on the highway. REAL ID rules require that each applicant for a driver's license or ID card must sign a declaration acknowledging that he understands any false statement in his application makes him subject to state and federal identity fraud statutes. Officials in states that have put this measure in place note that applicants will turn and walk out of DMV offices without signing the form, when they are confronted with reality of potential criminal prosecution. REAL ID clearly has a deterrent effect on would be fraudsters.

Thank you for the opportunity to submit this statement for the record.

The Coalition for a Secure Driver's License (CSDL), www.secure-license. org, is a 501 (c) (3) not for profit, crime prevention, educational charity incorporated in Washington, DC. CSDL conducts research and provides information that addresses public safety issues, fraud prevention benefits of stronger identity authentication procedures, and the issuance of counterfeit proof identity documents. CSDL essential research identifies best practices for DMVs, fraud detection and prosecution and related identity management topics. CSDL provides educational briefings and programs for communities and organizations throughout the United States. It is a national organization with over 10,000 members.

Coalition for a Secure Driver's License 1300 Pennsylvania Avenue NW, Suite 880, Washington D.C. 20004
Tel: (202) 312-1540

Mr. SENSENBRENNER. It is now my pleasure to introduce today's witnesses.

David Heyman is the Assistant Secretary for Policy at the U.S. Department of Homeland Security. Previously he served as a Senior Fellow and Director of the CSIS Homeland Security Program. He is an adjunct professor in security studies at Georgetown. He

received his Bachelor's degree from Brandeis University in 1986 and his Master of Arts from Johns Hopkins University School of Advanced International Studies in 1996.

Darrell Williams retired last year from the Department of Homeland Security after 38 years of Federal Government service. Prior to his retirement, Mr. Williams served as Senior Director for the DHS Office of State-Issued ID Support, formerly named the REAL ID Program Office. Prior to that, he served as the Senior Program Manager for the Department of Homeland Security Senior Border Initiative Program and Program Director for several U.S. Coast Guard command, control, and communications and Department of Defense programs. He received his undergraduate degree from Wright State University and his Master of Science degree in national security strategy from U.S. National War College. He received his Master of Public Administration degree from Central Michigan.

Stewart Baker is a Distinguished Visiting Fellow at the Center for Strategic and International Studies. He will shortly return to the practice of law at Steptoe & Johnson in Washington. From 2005 to 2009, he was the First Assistant Secretary for Policy at the Department of Homeland Security. Prior to that, he served as General Counsel of the WMD Commission and the National Security Agency. Mr. Baker received his undergraduate degree from Brown University and his J.D. from UCLA in 1976.

David Quam currently serves as Director of the Office of Federal Relations at the National Governors Association. Prior to his position at NGA, Mr. Quam was an associate at Powell, Goldstein, Frazer and Murphy, LLP. He held various other positions, including Director of International Affairs and General Counsel at the International Anti-Counterfeiting Coalition, Inc., and Majority Counsel to the Subcommittee on the Constitution, Federalism and Property Rights for the U.S. Senate Committee on the Judiciary. He received his Bachelor's degree from Duke and his Juris Doctor from Vanderbilt.

The witnesses' written statements will be entered into the record in their entirety. I ask that they summarize their testimony in 5 minutes or less. You see the blinking lights in front of you. Yellow means wrap it up. Red means time is up.

So I now recognize Mr. Heyman, and without objection, all of the witnesses' full written statements will appear in the record with their testimony.

TESTIMONY OF DAVID HEYMAN, ASSISTANT SECRETARY, OFFICE OF POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Thank you, Mr. Chairman, Congressman Scott, Chairman Smith, distinguished Members of the Subcommittee. I very much appreciate the opportunity to testify before you today and to discuss the progress that states have made implementing REAL ID and improving the security of driver's licenses and identification documents.

The Department of Homeland Security is fundamentally a law enforcement agency, and law enforcement must be able to rely on government-issued IDs and know that the bearer is who he or she

claims to be. Fraudulent IDs present opportunities for terrorists, and as such, securing IDs is a common sense national security and law enforcement imperative, and helps combat identity fraud and illegal immigration.

Since the Act was passed, we have made considerable progress. In 2007, DHS published an implementation plan, and in 2008 the Department published a final rule establishing minimum standards for states and territories. While the Nation's 56 states and territories have principal responsibility for implementing REAL ID, DHS has provided tangible support. Since 2007, the Department has awarded over $263 million in grants to fund enhancements to driver's license security programs and develop verification capabilities such as matching lawful status, improving facility security, modernization of information technology systems, increasing interoperability, and adding security features to documents.

Nearly half of this funding has been disbursed to states over the past 2 years. The fact that 54 of 56 jurisdictions have applied for and used these grant awards indicates that we share the same goals, objectives, and even standards for improving security of state-issued credentials.

One of the most challenging aspects of REAL ID is verifying source documents. When the bill was passed, those verification capabilities did not principally exist, particularly the ability to electronically match documents against appropriate Federal or other state databases. Over the past several years, DHS and states have collectively built and are building the technical infrastructure and systems to support verification of Social Security numbers, birth certificates, U.S. passports, and immigration status, all key steps toward improving the security of our documents.

Today I can report that significant progress has been made in this regard and in developing verification capabilities to meet the verification requirements, with all but one verification capability operational or in pilot testing today.

The Department's efforts extend beyond financial support. DHS has issued guidance documents and engaged stakeholders to ensure their concerns are being heard and challenges are being addressed. In 2009, DHS issued two guidance documents to assist states in understanding and meeting the REAL ID security standards, one on marked guidelines and another on best practices for security facilities and plans, card design, privacy and personnel security.

It was apparent from conversations with the states that additional clarification is warranted, and we will, in fact, be issuing additional guidance soon. This additional guidance will help reduce uncertainty regarding compliance by describing comparable programs that meet minimum standards, and this will help encourage states to submit information on their progress.

Additionally, our program office for this program has conducted considerable outreach through participation and meetings with states, territories, and partnering with Federal organizations. The office has conducted outreach to stakeholders, as well as attended a wide range of conferences, even visiting 44 of 56 states and territories and working extensively with the American Association of Motor Vehicle Administrators.

Perhaps the greatest success of REAL ID has been the security of driver's licenses has been improved in all states, even in the 13 states with legislation prohibiting REAL ID. The deadline for REAL ID is January 15th, 2013. Our goal is to get this done, and states have made significant progress in meeting the minimum security standards. All 56 states and territories have submitted documentation regarding their status with respect to material compliance benchmarks of REAL ID. They have made significant progress in meeting the benchmarks and other requirements, and most are meeting facility production issuance and card standards.

When determining whether a state has implemented a secure driver's license program, DHS will base its decision on the totality of what states have done. We commend them for their efforts. We have shared goals, and that is evident from the progress being made.

Thank you again for the opportunity to speak to you today, and I'm happy to answer your questions.

[The prepared statement of Mr. Heyman follows:]

Prepared Statement of David Heyman, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security

Chairman Sensenbrenner, Representative Scott, and Members of the Subcommittee: Thank you for your leadership on homeland security issues, and thank you for holding this important hearing today so that the Department of Homeland Security (DHS) can provide you with an update on the progress the states have made implementing the REAL ID Act of 2005, Title II of division B of Pub. L. 109–13 ("REAL ID Act" or "Act"). We welcome the opportunity to submit this testimony on how the state, territory, and federal partners have improved the security of driver's licenses and identification documents.

Over the last two Administrations, we have worked to implement the REAL ID Act of 2005. States have the principal responsibility for implementing REAL ID. DHS developed an Implementation Plan in June 2007 and published a Final Rule in January 2008, which provided states and territories with information on the minimum requirements that must be met and the funding available to help meet those requirements. Since then, DHS awarded over $200 million in grants to states and territories to fund enhancements to driver's license security programs. Additionally, DHS has issued guidance documents and engaged stakeholders to ensure their concerns were heard. DHS, the states, and the territories have collectively built or are building the technical infrastructure and systems to support verification of social security numbers, birth certificates, U.S. passports, and immigration status—key steps toward improving the security of our documents. Perhaps the greatest success of REAL ID has been that the security of driver's licenses has been improved in ALL states, even in the 13 states with legislation prohibiting their participation in REAL ID. Diligent outreach and work with states by DHS has yielded real benefits in the last several years.

In my testimony, I will elaborate on the progress but first it is important to provide the background to how we got to where we are today.

WHY WE NEED SECURE IDENTIFICATION DOCUMENTS

Law enforcement must be able to rely on government-issued identification documents and know that the bearer of such a document is who he or she claims to be. Obtaining fraudulent identification documents presents an opportunity for terrorists to board airplanes, rent cars, open bank accounts, or conduct other activities without being detected. According to the 9/11 Commission Report, "All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud." [1]

[1] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States,* at 390 (2004).

We recognize that preventing terrorists from obtaining these documents is critical. As the 9/11 Commission noted, "For terrorists, travel documents are as important as weapons."[2]

The 9/11 Commission recommended that the federal government work with other layers of government to solidify the security of government-issued IDs. While improving government-issued IDs alone will not thwart every planned terrorist attack, it does present an important obstacle to any potential terrorist operating in the United States and could aid law enforcement in stopping terrorist plots. Securing IDs is a common-sense national security and law enforcement imperative, which also helps to combat identity fraud and illegal immigration. The 9/11 Commission spelled out the need for the federal government and the state or territory[3] to take action together on this issue and together we have made considerable progress.

PASSAGE OF THE REAL ID ACT OF 2005

In May 2005, Congress enacted the *REAL ID Act of 2005* in response to the 9/11 Commission's recommendations for more secure standards for identification. The Act included the following provisions:

- Prohibits Federal agencies from accepting driver's licenses or identification cards unless the Department determines that the state or territory meets minimum security requirements.
- Establishes minimum standards for the:
  - Information and features that appear on the face of the card;
  - Physical security of cards to prevent tampering, counterfeiting, and duplication of the documents for a fraudulent purpose;
  - Presentation and verification of source documents, including presentation and verification of documents evidencing citizenship or lawful status; and
  - Physical security of production and storage facilities and for materials from which REAL ID cards are produced.
- Authorizes the Department of Homeland Security to make grants to states and territories to assist in conforming to the minimum standards of the Act.

In June 2007, DHS submitted, and the Senate and House Appropriations Committees subsequently approved, the *REAL ID Implementation Plan.* In the *REAL ID Implementation Plan,* DHS outlined its plans to make grant funds available specifically for projects that addressed the following areas:

- Enhancements to existing communications and verification systems to support cost effective electronic verification of source documents.
- Development of a secure indexing or pointer system for verification that an individual does not hold multiple licenses in multiple states or territories.
- Development of a cost effective capability for verification of lawful status. Improvements to the infrastructure to support electronic verification of birth certificates.
- Model privacy standards, security practices, and business rules regarding verification of applicant information with Federal and state agencies.

Additionally, in January 2008, the Department published the REAL ID regulation ("*Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*" (6 C.F.R. part 37)) providing greater detail on the minimum requirements states and territories must satisfy to be in compliance with the Act.

When determining whether a state has implemented a secure driver's license program, DHS will base its decision on what states have done to meet the requirements of the regulation. The security benchmarks in the regulation focus on: identity assurance procedures; license information and security features; secure business processes; employee training and background checks; and privacy protections. They also address the primary sources of fraud in the issuance and use of driver's licenses and identification cards.

---

[2] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States,* at 384 (2004).

[3] States and territories is used to refer to all fifty-six jurisdictions covered by the REAL ID Act, to include the fifty states, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Marianas Islands.

DHS FUNDING TO SUPPORT EFFORTS TO MEET THE SECURITY STANDARDS OF THE REAL ID ACT

Since FY 2006, the Department has obligated a total of $273 million in REAL ID program funds to support states and territories in their efforts to meet the requirements of the REAL ID Act.

From FY 2006 through FY 2011, FEMA awarded approximately $200 million in grants to 54 states and territories to fund individual projects to improve the security of their credentials, facilities, systems, and business processes commensurate with the standards of the REAL ID Act. States and territories have been able to allocate these funds based on individual needs, priorities, and operations.

States and territories have used these awards to meet the material compliance security benchmarks and other REAL ID standards, including:

- Adding tamper resistant or enhanced security features to their documents.
- Modifying their facilities to limit access to sensitive materials and card production areas.
- Modernizing information technology systems to promote interoperability.
- Conducting fraudulent document training or re-engineering the driver's license issuance process to reduce customer wait times.
- Implementing verification of lawful status.
- Improving their ability to protect applicants' personal information.

For example, using REAL ID FY 2008 Demonstration Grant funds, the State of New York purchased facial recognition software to detect individuals holding multiple drivers' licenses, sometimes in an attempt to evade law enforcement detection. New York used facial recognition technology to review the records of 600,000 holders of New York State Commercial Driver Licenses (CDLs). The results of this effort led to the arrest of more than 50 commercial drivers for fraudulently obtaining multiple driver licenses using an alias. Since February 2010, 800 people have been arrested for having two or more licenses under different aliases.

From FY 2008 through FY 2011, FEMA also awarded approximately $63 million in targeted grants to five states, Mississippi, Kentucky, Indiana, Florida, and Nevada, which volunteered to upgrade existing communications and verification infrastructure needed by all states and territories to meet the requirements of the REAL ID Act.

- The following verification capabilities to meet the verification requirements of the REAL ID regulation are either operational or in pilot testing. Specifically:
  - The states have upgraded the infrastructure necessary to support DMV verification of birth certificates. Birth records from 38 state Vital Records Agencies are now available for electronic verification;
  - Fifty states and the District of Columbia are verifying social security numbers;
  - Forty-seven states and territories have signed an agreement with USCIS to verify lawful status through the SAVE program; and
  - Four states are piloting verification of U.S. passports and this capability will be available to all states later this calendar year.
- Driver Licensing Agencies (DLAs) have used, and are continuing to use, remaining Driver's License Security Grant awards to fund the local information technology and business process improvements needed to connect to and use these systems.

Additionally, USCIS has supported almost $10 million in projects for the development and deployment of cost-effective methods that states and territories can use to verify lawful status, U.S. passports, and social security numbers. USCIS has worked together with the states and territories in the development, testing, and deployment of these capabilities.

FACILITATING CONFORMITY WITH THE STANDARDS OF THE REAL ID ACT—GUIDANCE AND OUTREACH FOR THE STATES AND TERRITORIES

The Department's efforts extend far beyond providing financial assistance to states and territories. DHS has been working with states and territories to assist them in understanding and meeting the security standards of the REAL ID Act. In 2008 and 2009, DHS issued two guidance documents for that purpose:

- *REAL ID Mark Guidelines* (October 2008), providing DHS recommendations for the marking of licenses.
- *REAL ID Security Plan Guidance Handbook* (February 2009), providing best practices for: securing facilities where enrollment, production, and/or issuance of REAL ID driver's licenses and identification cards occur; card design and security; privacy; personnel security, and the contents of the security plans.

Because of additional requests from the states for clarification, the Department plans to issue additional guidance in the near future to clarify the minimum standards that states and territories must meet to achieve full compliance with the Act and provide examples of how states can meet them. While DHS has worked closely with many individual states and territories—some of which already submitted full compliance packages—the Department believes that the guidance will reduce the uncertainty surrounding the regulation and encourage states and territories to submit information on their progress consistent with the minimum standards of the REAL ID Act. In providing further guidance, DHS's purpose is to afford every state and territory the flexibility and opportunity to reach full compliance in a practical manner.

DHS's subject matter experts have worked with the states and territories continually since 2007. Through its participation in meetings with the states, territories, partnering federal organizations, and stakeholders as well as attendance at a wide range of conferences, our program office, the Office of State-Issued Identity Support (OSIIS), visited 44 of 56 states and territories covered by the REAL ID Act, including four of the five U.S. territories. DHS continues to work closely with the Department of State on the passport verification module. DHS has worked with the American Association of Motor Vehicle Administrators (AAMVA) to coordinate implementation of the standards of the REAL ID regulation. In particular, DHS participated with the states and territories in the drafting of the *Personal Identification—AAMVA North American Standard—DL/ID Card Design* to ensure that states and territories can implement the REAL ID requirements for card design by means of common, consensus-based data formats and card technologies endorsed by all states and territories.

Since 2007, OSIIS has also participated in at least 40 meetings with AAMVA and member states regarding all aspects of the REAL ID program, and provides regular briefings at the semiannual AAMVA Board of Directors Meetings and regional meetings. OSIIS representatives have also attended annual meetings of National Association for Public Health Statistics and Information Systems since 2007. The program communicates regularly with the Coalition for A Secure Driver's License. OSIIS has also participated in a dozen on-site meeting with the State of Mississippi and the Mississippi consortium of states leading state efforts to improve the communications system infrastructure supporting the verification requirements of the Act.

Thirteen states[4] have laws prohibiting compliance with the REAL ID Act. Even so, DHS believes that some of these states already issue secure identification documents consistent with the standards of the regulation.

It is important to note that the REAL ID regulation provides DHS with the ability to recognize comparable programs in states and territories that issue driver's licenses and ID cards consistent with the minimum requirements of the regulation. States and territories are, in fact, already achieving success with their comparable efforts.

For example, four states (Michigan, New York, Vermont, and Washington) currently issue Enhanced Driver's Licenses and Enhanced Identification Documents (EDLs) that were developed in alignment with the REAL ID standards, but can also be used by U.S. citizens as a border crossing document to enter the United States through a land or sea port of entry in accordance with the Western Hemisphere Travel Initiative (WHTI).

APPROACHING DEADLINE

The deadline for meeting the standards of the REAL ID Act is January 15, 2013. To assist DHS in making compliance determinations, the regulation also requires states and territories to submit certification materials at least 90 days prior to the effective date of compliance. A DHS compliance determination means that a state's or territory's program meets or exceeds the REAL ID regulatory requirements or has a program comparable to the requirements of the REAL ID regulation.

[4] Alaska, Arizona, Idaho, Louisiana, Maine, Minnesota, Missouri, Montana, New Hampshire, Oklahoma, Oregon, South Carolina, and Washington.

CONCLUSION

This hearing seeks to take stock of implementation of the REAL ID Act of 2005. DHS relies on alternative data collection methods, such as grant reporting, to document progress made by states and territories in improving the security of their driver's licenses and identification cards commensurate with the standards of the REAL ID Act. While this does not afford DHS full visibility into all the progress states have made, we can say that the Department, along with our federal, state and territory partners, has made great strides in improving the security of credentials since 9/11 and the subsequent enactment of the REAL ID Act of 2005. States and territories have made significant progress in meeting the benchmarks and other requirements of the REAL ID regulation and most are meeting REAL ID facility, production, issuance, and card standards. We commend them for their efforts.

Thank you again for this opportunity to testify. I am happy to answer any questions you may have.

Mr. SENSENBRENNER. Thank you very much.

Mr. Williams?

TESTIMONY OF DARRELL WILLIAMS, FORMER SENIOR DIRECTOR, OFFICE OF STATE-ISSUED ID SUPPORT, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WILLIAMS. Mr. Chairman and Ranking Member, and distinguished Members of the Subcommittee, thanks for the invitation to actually speak.

From 2006 until when I retired in 2011, I was the Director for the REAL ID program. Pretty much all the documents, the concept of operations, implementation plans, the expenditure plans I pretty much developed with my staff. All the staff that is currently in the office I actually selected.

In regards to the implementation of REAL ID, which is what I will focus on, we actually established an outreach program which included all 56 states and territories in regards to our attempts to, first of all, help them understand what REAL ID is and does, but also to take a look at the implementation activities associated with REAL ID so they could actually get better cost estimates as they looked forward to attempting to implement the program.

A lot of the successes that REAL ID has actually come to know really came from the states leaning forward not so much because of what DHS did but because the states realized long before 9/11 that there was a number of fallacies within their processes in regards to security dilemmas in their facilities, and then they also realized that a lot of the security issues associated with producing a driver's license actually came from internal processes where their individuals created a lot of the internal fraud.

So again, those are things that states realized, states wanted to do, and then REAL ID actually became the overall umbrella to help states implement the kinds of things they wanted to do and actually start off with.

The progress that states have made has been well documented. For example, if you take a look at states, and we actually did a state survey where a number of states responded, 82 percent of states have improved their card security. All those security improvements are really consistent with REAL ID. There are a number of other stats that I have in my testimony that I won't review now. But again, it shows again the tremendous progress that states

have made and that states are committed to improving their security and the integrity and the trustworthiness of their documents.

One of the things that has prohibited states from making more progress is states need clear and consistent guidance. That is the one thing that they have not received. For example, with the PASS ID dilemma, states became confused as to whether or not DHS was going to implement REAL ID or replace it at some point in time with PASS ID. In that confusion, states decided to stop using some of the grant funding to improve the security of their systems. That took, in some cases, anywhere from 12 to 18 months longer.

The other example is we talk about the verification capabilities that states will need to use to verify whether or not a person is issued a driver's license in another state. That system, which I really started to develop back in the 2007 timeframe, with the advent of the PASS ID confusion, that progress was also delayed. So that IT system that is not in progress today could have been furthered if states weren't in that confused state waiting for DHS to provide clear and consistent guidance.

The other guidance that states aren't totally sure of is when states take a look at the REAL ID Act and what it requires, it does not provide clear pass/fail guidance as to what states need to evaluate their facilities, their people, and their processes to clearly determine whether or not they meet the requirements of the REAL ID Act. DHS also does not have that pass/fail criteria.

So when we talk about compliance audits at some point in time in the future, without that clear pass/fail criteria, DHS would not be capable of actually rendering and determining whether or not a state actually meets the requirements of the Act itself.

There is more to say, and I will save much for the questions so I can stay within the 5 minutes. But again, thanks for the invitation to speak, and I look forward to your questions.

[The prepared statement of Mr. Williams follows:]

Prepared Statement of Darrell Williams, former Senior Director, Office of State-Issued ID Support, U.S. Department of Homeland Security

Chairman Smith, Ranking Member Conyers, and distinguished members of this Subcommittee I am pleased to be here today to discuss the importance of the REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards.

From December 2006 until 1 April 2011 I served as the Director for the Department of H0meland Security (DHS) REAL ID Program Office, later renamed the Office of State-Issued ID Support. During my tenure, I established the REAL ID Program Office, planned and executed the program's budget and selected each member of the REAL ID program office team. In addition, I lead the development the of REAL ID Regulation, REAL ID Program's Concept of Operations, and the REAL ID Implementation and Expenditure Plans which were both approved by DHS and submitted to Congress. I specifically communicated the program's requirements, implementation progress and expenditures to DHS executive leadership, Office of Management and Budget and Congress. I also worked with other Federal agencies and developed an outreach program designed to establish and maintain a long-term partnership with all U.S. States and territories Department of Motor Vehicle (DMV) leadership, the American Association of Motor Vehicle Administrators (AAMVA) and specific document identity data verification system managers. My goal was simply to assist states to enhance the security, integrity and trustworthiness of their driver licenses and identification cards, facilities and processes to comply with the requirements of the REAL ID Act and implementing regulation.

A brief synopsis of the primary requirements are located in Section 202 of the REAL ID Act which reads, "Prohibits Federal agencies from accepting State issued driver's licenses or identification cards unless such documents are determined by the Secretary to meet minimum security requirements, including the incorporation

of specified data, a common machine-readable technology, and certain anti-fraud security features. In addition, Section 202 also sets forth minimum issuance standards for such documents that require: (1) verification of presented information; (2) evidence that the applicant is lawfully present in the United States; (3) issuance of temporary driver's licenses or identification cards to persons temporarily present that are valid only for their period of authorized stay (or for one year where the period of stay is indefinite); (4) a clear indication that such documents may not be accepted for Federal purposes where minimum issuance standards are not met; and (5) electronic access by all other States to the issuing State's motor vehicle database."

Prior to managing the REAL ID program, I served as the Senior Program Manager for the DHS's Secure Border Initiative Program, several U.S. Coast Guard Command, Control and Communications programs and numerous Department of Defense major weapon system acquisition and support programs. Lastly, among other degree's, I have a MS Degree in National Security Strategy from The National War College.

Although I am be delighted to discuss or address any questions the Committee may have regarding the REAL ID Act or Regulation, I will focus my written testimony and opening remarks on the program's implementation activities.

Under my direction the REAL ID Program Office, later renamed the Office of State Issued Identification Support, was responsible for REAL ID program development, REAL ID Rule development, REAL ID related grant oversight, development of an identity documentation electronic verification capability and implementation of the REAL ID Act. The regulatory scope of the REAL ID Act and regulation include the following:

- Approximately 240 million holders of State driver's licenses and identification cards
- 56 jurisdictions, including the 50 States, the District of Columbia, and five U.S. territories
- Approximately 2,200 State DMV offices and facilities employing about 30,000 state employees and contractors
- Millions of commercial airlines travelers and visitors to the Federal facilities
- Multiple Federal agencies to include Department of Transportation, the Transportation Security Administration (TSA), Federal Protective Service (FPS), the Nuclear Regulatory Commission (NRC), and other Federal entities managing access to Federal facilities.

In December 2006 one of the most formidable REAL ID challenges facing DHS was direct opposition by the states and specifically each state's DMV Offices. During this time frame, the states DMV administrators collectively considered DHS an absolute adversary and as result the few discussions that occurred between representatives from the state DMV offices and DHS were quite contentious and non-productive. However, I'm delighted to report that upon my retirement in 2011, numerous DMV staff members and specifically DMV administrators from across the country and the U.S. territories emailed, phoned and sent letters to thank me for my efforts that led to establishing and maintaining an open and honest REAL ID implementation partnership.

The benefits of this partnership which began in the spring of 2007 eventually resulted in the DMV administrators teaming with AAMVA to become the REAL ID Program Office's most supportive implementation advocate. The implementation success that will be discussed later in this testimony would have not been realized without the DMV administrators and AAMVA support.

An example of this support was first realized in the spring and summer of 2007, when AAMVA agreed to host four regional meetings in the cites of Baltimore, Chicago, Los Angeles and Atlanta which allowed me to conduct 4 four hour meeting with all the DMV staff members in each region to discuss DHS plans regarding the proposed REAL ID rule and address the numerous misconceptions, false information and reduce the DMVs fear of this unknown rule's impact on how they conduct their day to day business with their respective customers.

In addition to support, AAMVA and the state DMV's funded their personnel expenses to attend and participate in these meetings. These meetings resulted in a tremendous amount of clarity for the states. This initial series of regional meetings reduced the state's high anxiety by clarifying the rules intensions, removing misinformation and asking the states to share their operational insight.

While at these meetings I also conducted several side-bar meetings with DMV regional leaders. From the follow-on side bar meetings I recruited numerous state

DMV staff members to partner with DHS to form several working groups. Early in 2007, I realize that I did not have the program funding or adequately trained staff to properly understand all the relevant operational aspects of the state DMV driver's license issuance processes, facilities and IT capabilities. To quickly acquire the technical expertise needed, I partnered with the DMV leadership to develop several DMV process-focused technical working groups comprised primarily with the DMV and AAMVA staff members. AAMVA agreed to host the working group meetings. Without belaboring the point, I bring this information forward to stress that virtually all the implementation progress made to date has been greatly facilitated with state DMVs and AAMVA technical, administrative assistance and in some cases financial support.

States have been fully engaged in improving the security, integrity and trust worthiness of their respective state issued driver's license and identify cards. Many of these security improvements either exactly meet or are consistent with the requirements of the REAL ID Act or Rule. States have made these improvements primarily because they were well aware prior to September 2011 that their driver's license and identity card issuance processes, cards and facilities had numerous security deficiencies. In addition, states have long wanted to develop a capability that allows each state's DMV to electronically verify all applicant's identity documents (birth record, passport, out-of-state's driver's license, immigration documents) information prior to issuing a driver's license or identity card.

States have and continue to make significant implementation progress consistent with requirements of REAL ID. A February 2011 Driver's Information Verification System (DIVS) report shows the results of a state-based questionnaire where states self-report their driver's license and identity card security progress as follows:

- 82% of states have improved their card security
- 96% of states provide fraudulent document security recognition training
- 89% of states perform background checks on employees
- 78% of driver's license agencies have improved the physical security of their facilities
- 96% of states have instituted IT hardware and software that links a given license issuer with a given issued license
- 71% of states access USCIS data to verify U.S. issued immigration documentation
- 84% of states coordinate driver's license and identity document expiration date to an applicant's U.S.-issued immigration documentation.

The above DIVS report indicates the great progress states have made absent clear and consistent DHS guidance. DHS vacillation on support of PASS ID vs. REAL ID temporarily delayed numerous states from making progress and resulted in an untimely delay in states utilizing their grant funding to make security improvements. In 2010, numerous states expressed concern that if they continued to expend their 2008 and 2009 grant funds to comply with REALID requirements, those funds would not be available if the requirements were changed to align with PASS ID. In absence of clear and consistent guidance, numerous states delayed grant fund expenditures and thus REAL ID implementation enhancements. States remain unclear if DHS will, yet again, postpone the compliance deadline beyond January 2013, continue to pursue PASS ID or another alternative, or if they should march full speed ahead to continue to improve and enhance their driver's license and identity card issuance processes to become comparable to or consistent with REAL ID requirements.

In addition, states continue to express concern about REAL ID Rule Subpart E.37.51 that says "States must have met the REAL ID Rule standards of subparts A through D or have a REAL ID program that DHS has determined to be comparable to the standards of subparts A through D." To date, DHS has not provided states clear guidance on what constitutes comparable and must do so as soon as possible to allow states time, if they so elect, to pursue a comparable alternative lead time away from the established compliance deadline of January 15, 2013.

In addition to the above, below you will find a list several other implementation issues that should be resolved as soon as possible to provide all willing states a realistic opportunity to achieve a successful REAL ID program implementation.

- DHS must establish clear pass/fail criteria that states can use to measure and determine when they comply with the REAL ID or comparable program compliance requirements.

- Until such clear guidance is provided, states do not have the ability to determine if they have met all the requirements for compliance.
- In addition, DHS will need the pass/fail criteria to perform future compliance audits

- Per REAL ID rule section 37.55, 37.59 and 37.61, DHS must establish a state compliance audit process to conduct future compliance audits. A compliance audit process is required to verify if a state has met or is meeting the required initial or recertification compliance requirements per the REAL ID rule.
  - Subpart E—Procedures for Determining State Compliance, section 37.55 indicates that DHS will make a final compliance determination. Subpart E—Procedures for Determining State Compliance, section 37.59 indicates that DHS will review to determine whether the state meets the requirements for compliance.
- DHS must develop a REALID enforcement strategy that clearly conveys how the REAL ID Act requirements will be enforced beginning January 15, 2013.
  - Enforcement strategy must include at minimum the Federal Protective Service, Transportation Security Agency and other Federal facilities as covered by the REAL ID Act and implementing regulation.
- DHS must develop a grant funding financial audit review strategy to ensure the grant funds awarded to states are being expended in accordance with the grant application and approval.
  - Currently, DHS lacks the process to know and ensure accountability for REAL ID grant funds expenditures
- To vastly improve the quality of program implementation, strongly encourage the REAL ID program be transitioned to an operational environment that has acquisition, program management, system engineering, at a minimum, as core competencies. Although the DHS Office of Policy may be well intended, the office is not equipped with the experience or expertise to oversee the design and development of an operational program. The Office of Policy is especially not capable and does not have the expertise to oversee the design, test, implementation an initial operation of the multi-million dollar REAL ID Driver's License Information and Verification (DIVS) Program which is currently in the design phase. This REAL ID electronic document verification program, developed with Congressional appropriated funds, is currently in the design phase. The REAL ID program has been in the implementation and system development stage for several years. For example, for past three years the Office of Policy has overseen and managed the requirements generation process, which will lead to the design, development, testing and fielding of an operational IT system expected to process millions of daily state to state DMV transactions. The DIVS system is expected to complete the design phase in 2014, testing in 2015 and become operational and deployed by 2016. Just as policy should not be developed in an operational environment, an IT focused system's design, development, test, initial operation and full system deployment should not be led by a Policy Office.
- REAL ID's Greatest implementation assets:
  - All DMV leadership is aware of the critical need to improve the security, integrity and trust worthiness of their driver's license and identity card processes and they are willing to take action.
  - State's continue to make significant progress to enhance the security of their cards, systems, processes and facilities
- REAL ID's Greatest implementation impediments:
  - Retaining the design, development, testing and fielding of an operational program in a Policy making environment will continue to delay the program's implementation. The program must be transitioned to an operational environment.
  - Lack of DHS clear and consistent guidance to states.
    - The program lacks clear pass/fail compliance criteria
    - The program lacks clear guidance on what constitutes a comparable program

- The program lacks clear guidance on how enforcement will be implemented and if enforcement will begin January 15, 2013

○ Lack of DHS executive level engagement and support

- States DMV leadership remain uncertain and unconvinced that DHS executive leadership is committed to REAL ID implementation

---

Mr. SENSENBRENNER. Thank you, Mr. Williams.
Mr. Baker?

TESTIMONY OF STEWART A. BAKER, PARTNER, STEPTOE & JOHNSON, LLP

Mr. BAKER. Chairman Sensenbrenner, Ranking Member Scott, Chairman Smith, Chairman Emeritus Conyers, Members of the Committee, it is a pleasure to be here. My claim to fame is I hired Darrell and had David Heyman's job before he had it.

It is a pleasure to talk about this topic because it is so important. It is not just that the 9/11 Commission after 10 years reiterated how important it was. It is not just that practically every terrorist act in the last 20 years, from Oklahoma City to 9/11 to the Lubbock, Texas attacks, depended on fake and fraudulent IDs. But one person, one household in 14 every year is the subject of identity theft. Most of it, the most serious of it is facilitated by fake IDs. This is the real privacy issue that we should be focused on. People are losing control of their identities to people who have easy access to fake or fraudulent driver's licenses.

The good news that I do want to talk about is that most states have, at the end of the day, as we have heard already, recognized they have a responsibility to fix their security problems, and nearly 40 of them could meet this deadline, or perhaps more. They are on track to meet the deadline. That is great news. It is particularly impressive that they have put in place the ability to check birth certificates, which are really the most dangerous breeder document that facilitates this kind of fraud. That is possible by January of 2013.

The bad news from my point of view is that even if 80 or 90 percent of the states meet this deadline, they are not going to get rid of 80 or 90 percent of the fraud. They are going to get rid of about 10 percent of the fraud because the fraudsters and the terrorists, everybody who wants a fake ID, are just going to figure out which states allow them still to use bad birth certificates or to meet other fraudulent requirements, and they are going to go there.

So until we get everybody up to a high level, we are not going to solve this problem. That is why, I think, the REAL ID Act very wisely put in place a penalty for failure to meet this deadline. Until the last state comes on board, we have a problem in our ID system.

The difficulty with the penalty that we have, and I faced this because I actually was facing the prospect of pulling the trigger on the refusal to accept licenses at airports, is it is like a nuclear weapon. It is really effective at scaring people, but when you actually set it off, a lot of bad things happen that no one really wants to see happen.

So there is a kind of chicken that is played between the Department and the states. The states say, "I wonder if they will really

set that off, because if they won't, maybe I can just, you know, skate past the deadline." And the Department doesn't want to set it off, but they have to persuade people that they are actually going to do something serious when the deadline arrives. I don't think David or the Administration has persuaded anybody that they are serious about setting off that weapon or imposing that penalty.

So my suggestion for this committee is you really need to find some penalty to enforce that deadline that is not dependent on the Secretary having the will to use that penalty, and my suggestion in the testimony—I will stop here—is that you say to the 54 or 56 jurisdictions who took money to comply with REAL ID that if you don't meet January 2013, give the money back. Thanks.

[The prepared statement of Mr. Baker follows:]

Prepared Statement of Stewart A. Baker, Partner, Steptoe & Johnson LLP

Chairman Sensenbrenner, Ranking Member Scott, Members of the Subcommittee, I am pleased to testify today about the importance of improving the security of drivers' licenses, the identity documents on whose security Americans rely daily.

WHY WE NEED MORE SECURE DRIVERS' LICENSES

It shouldn't be necessary to say that we need secure identification documents in the United States. Ten years ago, the 9/11 hijackers exploited the security weaknesses of state DMVs to obtain nearly 30 licenses, many of them by fraud. And twenty years ago, Timothy McVeigh used a fake South Dakota license to rent the truck he filled with fertilizer and fuel oil; South Dakota's license security was so weak that McVeigh made his fake license with a typewriter and a clothes iron.

That's not the end of it. Last year, the FBI arrested a Saudi student in Texas whose notes showed that he had devoted much of his young life to winning a scholarship to the United States, where he planned emulate Osama bin Laden by killing large numbers of Americans. His plans included casing the home of George W. Bush and preparing a chronology for the attacks listing these key steps in his plan: "obtaining a forged US birth certificate, applying for a US passport and driver's license; . . . using a different drivers' license for each car he rents; . . . putting the bombs into the cars and taking them to different places during rush hour."

Some things never change. Terrorists hoping to attack us at home will keep exploiting the insecurity of our drivers' license system for as long as we fail to improve that system.

So will criminals. Identity theft is a fast-growing and disturbingly common crime; one household in 14 suffered an identity theft in 2010, according to the U.S. Justice Department, up from one in 18 just five years earlier. Some of the most intrusive and devastating forms of identity theft—forged checks, for example, or employment fraud—require a fraudulent drivers' license or similar identification document to accomplish. Bad drivers' license security has victimized millions of Americans.

It could even get some of them killed. I am still appalled by the story of Kevin Wehner. Having his wallet stolen on vacation was the beginning a nightmare. The thief used Wehner's documents, along with a forged Virgin Islands birth certificate, to obtain a Florida license in Wehner's name. When Wehner moved to Florida, the DMV refused to give him a license. "You've already got one," they told him. He sent them his picture to straighten out the mess. That only made things worse. Because the identity thief had moved on to stealing cars and killing police officers. To catch the killer, Florida police circulated the photo that the real Kevin Wehner had recently supplied to the DMV. Luckily, a friend who saw the photo on TV called Wehner before a nervous police officer pulled him over. Shortly thereafter, police located the fake Kevin Wehner and shot him dead in a gun battle. Florida's inability to check a forged birth certificate could have killed the real Kevin Wehner just as easily.

WHY REAL ID HAS NOT YET BEEN IMPLEMENTED

Unfortunately, not everyone agrees with the need for better drivers' license security. Opposition to REAL ID unites the nations' governors and the ACLU. As a candidate, President Obama campaigned against REAL ID. And as a governor, Secretary Napolitano did the same. So it was no surprise that the Obama administration supported repeal of REAL ID and adoption of a softer approach, called PASS

ID. Expecting PASS ID to be adopted, the administration soft-pedaled the states' obligations under REAL ID.

But PASS ID did not pass, and REAL ID is still the law. Unfortunately, however, it's not being treated like a real law. In 2009, the Secretary of Homeland Security permanently stayed the deadline for states to come into material compliance, on the grounds that the Department was pursuing PASS ID. By March 2011, with the deadline for full compliance with REAL ID just two months away, that reasoning wouldn't work anymore; everyone recognized that PASS ID was dead. But the Secretary nonetheless postponed the deadline for full compliance to January 2013 without taking comments. The remarkable justification for the delay was that the administration had encouraged the states to hope that the law would change, so they didn't take steps to comply with the law as it stands:

> [S]ome States delayed investing in new technology and process changes because of uncertainty associated with Congressional action on the PASS ID Act. PASS ID, which was supported by the Administration as well as State associations, including the National Governor's Association and the American Association of Motor Vehicle Administrators, would have modified certain requirements of REAL ID to facilitate State compliance. States delayed making investments to implement REAL ID to ensure they were not making expenditures to comply with requirements that would have been undone had PASS ID been enacted into law. Now that PASS ID seems unlikely to be enacted, DHS anticipates States will refocus on achieving compliance with the REAL ID requirements.

Wow. I only wish I could get an extension on my tax return by saying I was hoping the law would change before the returns were due but that I'm now ready to "refocus on achieving compliance" with the requirements of the tax code.

In fact, apart from hoping that the states will refocus, the Department does not seem to be doing much to encourage them to meet the new deadline. As far as I can see, it hasn't audited state compliance; it hasn't processed the submissions of states that want to certify their compliance with REAL ID; and it hasn't pressed the states that are lagging far behind to step up their efforts.

THE 9/11 COMMISSION IS RIGHT: WE CAN'T AFFORD MORE DELAY

That approach will mean years of delay in improving drivers' license security, millions more victims of identity theft, and perhaps more victims of terrorism. It will mean negating not just a federal law but one of the last unimplemented recommendations of the 9/11 commission. The members of that commission recently reassembled for a tenth anniversary review of the nation's progress in adopting its recommendations. They were blunt in their criticism of the administration's delay in implementing REAL ID:

> Recommendation: "The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses."
>
> . . .
>
> [T]he deadlines for compliance have been pushed back twice . . . until January 2013. The delay in compliance creates vulnerabilities and makes us less safe. No further delay should be authorized; rather, compliance should be accelerated. The delay in compliance creates vulnerabilities and makes us less safe. *No further delay should be authorized; rather, compliance should be accelerated.* (Emphasis added.)

The 9/11 Commission members are right. The foot-dragging should stop, in Washington and in the states.

MOST STATES ARE READY TO MEET THE REQUIREMENTS OF REAL ID

This is particularly true because, despite all the public outcry and political posturing, most motor vehicle departments are making good progress toward the goals set out in the REAL ID act. Janice Kephart of the Center for Immigration Studies has done invaluable work in surveying the states' progress toward achieving compliance with the standards set by REAL ID. Her most recent study estimates that nine states are on track to achieve full compliance with all REAL ID requirements by January 2013, and that another 27 will have achieved material compliance with the act by then. That means that the great majority of states can meet the deadline, at least for material compliance, if they simply keep on doing what they have been doing.

In saying that, I do not mean to overlook the distinction between material compliance and full compliance. The principal difference is that states can achieve mate-

rial compliance without having in place an electronic verification system for birth certificates. To achieve full compliance, they must check birth certificates with the issuing jurisdiction.

Now, as you might guess from my early remarks, I think that checking birth certificates is crucial to achieving a more secure license system. Birth certificates are much easier to forge and much harder to check than licenses, so it's no wonder that everyone from aspiring terrorists to cop-killing car thieves views a forged birth certificate as the key to building a fake identity.

And so, having an electronic system for checking birth certificates is crucial. It too should be in place as soon as possible.

BIRTH RECORDS CAN BE CHECKED ELECTRONICALLY TODAY

Once again, there is good news on this front in the Kephart report, which says that by February of this year, 37 states had already entered their birth records into a system that allows other agencies to conduct verification online. This system, called Electronic Verification of Vital Events (or EVVE), is administered by the National Association for Public Health Statistics and Information Systems (or NAPHSIS). The network is still growing; NAPHSIS tells me that they've added another state since February; EVVE now covers 38 states. And the system isn't just theoretically available. It's actually being used on a daily basis by several US government agencies, such as the State Department's passport fraud investigators, the Office of Personnel Management, and the Social Security Administration.

The really good news, then, is that there are no technical barriers to nearly immediate implementation of electronic birth certificate checks. Any state that can achieve material compliance by 2013 can also achieve the most important element of full compliance by that date; it just has to hook up its DMV to EVVE. In short, nearly 40 jurisdictions are on track to do what the 9/11 Commission recently urged them to do: implement drivers' license security without delay.

WHY CONGRESS NEEDS TO ACT

Now let me turn to three pieces of bad news, and the reason that the 9/11 Commission's goal will remain unfulfilled unless Congress acts.

1. Everyone's security is set by the weakest states, not the strongest. First, the efforts of nearly 40 jurisdictions to improve their license security won't do us much good unless the remaining states get on board. It's become quite obvious that identity thieves—whether they're illegal workers or fraudsters—keep a close eye on the license security practices of the states. When they need a fraudulent document, they always manage to find the states with the weakest security.

This is why REAL ID was needed in the first place. Many states did a good job, and a few did not; but those few undermined the efforts of all the others. We have to bring the laggard states up to the same standards that most states are on track to meet. Only a firm deadline, with penalties, will do that. And, since the administration has made clear its reluctance to enforce REAL ID, Congress needs to impose its own deadline.

2. We need new penalties for noncompliance. That brings me to the second piece of bad news. The main penalty for states that miss deadlines is that TSA will refuse to accept the licenses they issue, meaning that residents of those states won't be able to fly without a U.S. passport or other strong ID. The problem with this penalty is not that it's too weak.

Rather, it's too strong. It's like a nuclear weapon—so big and so damaging to so many innocent people that whoever sets it off is likely to be judged harshly. With both sides aware of the risks, REAL ID penalties are at best a game of chicken between recalcitrant states and DHS. If the states convince DHS that they will not meet the deadline, DHS will probably cave and issue an extension. If DHS convinces the states that real penalties will be imposed and the deadline will not be extended, then the states will probably cave and come into compliance. But to be candid, having granted two extensions already, I don't think this administration can persuade the states that this time is different.

That's why Congress should act. REAL ID needs a statutory deadline with penalties that are credible. Here's one idea. Remember that the states, almost without exception, have accepted more than $220 million in grants to comply with REAL ID or improve license security; they accepted grants during fiscal years 2005, 2007, 2008, 2009, and 2011. Many of those grants required the states to affirm that they were in the process of complying with REAL ID. Yet years later some of them still are not on track to meet the much-delayed implementation deadline. This raises the question whether the lagging states took federal grant funds in good faith and

whether they spent the funds prudently. If they lag so badly that they miss even the January 2013 deadline, perhaps it's time for them to give the money back.

So here's one idea for changing the dynamic of REAL ID enforcement: perhaps any future appropriations or authorization bill dealing with homeland security, terrorism, or immigration should include a provision requiring that states failing to meet the REAL ID deadline must return any funds received to improve drivers' license security. The paybacks could be cumulative, increasing over time so that the states have a growing incentive to comply. While imposing fines on states or a requirement to disgorge grant funds would raise legal concerns, I see no bar to automatically reducing by the amount of the penalty any future payments that would otherwise be due to states under other programs. Such a penalty would also respond to the current budget climate by reserving scarce federal funds for states that live up to their obligations under federal law. It could be implemented either through appropriations or authorization bills. That's the kind of modest but credible penalty that is likely to finally break the last logjam of lagging states and bring about nationwide license security.

3. Electronic birth certificate checks probably won't happen without enforcement of the deadline. Finally, the last piece of bad news concerns the birth certificate network, EVVE. As I said, it is available and ready for states to use. But the states are not in fact using it, at least not to check birth certificates from other states. (Some states do use the system to check their own birth records.) Indeed, a pilot in which three states were using EVVE to do cross-border birth record checks has recently ended, and the states involved decided not to continue the checks—a troubling bit of backsliding, given the importance of birth certificates as breeder documents for false IDs.

Why are states reluctant to use EVVE for drivers' license checks? I suspect the problem is the cost of the service. When the system is running at low volumes, as it is now, the cost of an electronic record check on EVVE is nearly two dollars. That's a lot of money for states that issue tens of millions of licenses and may charge only $20 or $30 for each one. States have an incentive to hang back and let other states pay the high cost of being an early adopter.

This Alfonse-and-Gaston problem is easy to solve. If all state motor vehicle agencies join EVVE at the same time, its volume pricing will bring the cost of each check down to less than a dollar—94 cents, I'm told by NAPHSIS. We can achieve this goal if DHS simply enforces the existing deadline of January 2013. Overnight, the cost of the service will drop. That is another reason to impose a deadline and to include birth record checks.

I know the states have complained about the costs of REAL ID. That complaint makes no sense in the context of EVVE, however, because most of the 94-cent cost goes to state vital records agencies to cover their costs of maintaining EVVE records. Let me say that again; roughly 87 cents of the 94-cent EVVE fee is simply a transfer between state agencies—from state DMVs to state vital records offices. Even when those transfers cross state boundaries, they go in both directions and are likely to roughly balance out.

It turns out that the states will be literally paying the great bulk of EVVE fees to themselves, and their reluctance to make these payments is simply a disguised turf war between the DMVs and the vital records offices. Surely we should not leave future victims of future identity thefts and terrorist acts unprotected simply because two state agencies do not agree on which of them will pay to maintain digitized birth records.

Still, if Congress wants to help the states achieve compliance by further lowering the cost of birth record checks, there is a way to do that while also making the country more secure. As I understand EVVE's pricing, its lowest fees will be charged to all comers once volume in the system exceeds 1.2 million checks a month. Bringing all the states on board through REAL ID will achieve that end. But so will requiring that the State Department check all birth certificates through EVVE before issuing a passport. Today, I believe, State only checks a limited number of certificates through EVVE, as part of its fraud prevention program. If it checked all certificates through EVVE, it would likely uncover more fraud, and it would lower the cost of such checks dramatically for all. This would add to the State Department's costs, but not to the deficit, because the cost of passport processing measures is recovered by passport fees.

CONCLUSION

Making sure that Americans can rely on the security of their drivers' licenses is a vital national priority. It has been stalled for too long, and this hearing serves

an important purpose in drawing attention to how much has been achieved and how much still remains to be done.

Thank you for the opportunity to testify here today.

Mr. SENSENBRENNER. Thank you, Mr. Baker.

Mr. Quam?

TESTIMONY OF DAVID QUAM, DIRECTOR, OFFICE OF FEDERAL RELATIONS, NATIONAL GOVERNORS ASSOCIATON

Mr. QUAM. Thank you, Mr. Chairman, Mr. Scott, Mr. Smith, Mr. Conyers, Members of the Subcommittee. It is a pleasure to be here on behalf of the National Governors Association on an issue that governors have worked on for a very long time.

I think there is some good news here that you are hearing. States have made progress, considerable progress in moving ahead. Every governor is concerned with increasing the integrity and security of their driver's licenses. They were in 2005, 2007, 2009. They are interested in that issue today. Fraud, theft, security are all concerns for every governor.

And because of that, governors, when they started to address both REAL ID and the regs as they came out, looked through a lens of some core principles, that licenses and identification cards should accurately reflect the identity of the owner, that the laws and regulations should facilitate and encourage participation by all jurisdictions, that those laws and regulations should also enhance the security and integrity of all licenses and ID cards while retaining state flexibility to innovate, set a floor, let states go above it, and then address critical privacy concerns while reducing or eliminating unnecessary cost.

Part of the delay with REAL ID, as it was initially written and as it came out, represented an unworkable and unfunded mandate, a very serious challenge for states. What we need is continued flexibility in implementation if we are going to meet the core objectives of the Act, something that I think governors share with this committee and with Congress, and the Department of Homeland Security.

So where do we stand? Mr. Chairman, you accurately stated exactly where states are today. Six states have submitted full compliance certifications. Twenty-two states have said that they are materially compliant. Four states are using enhanced driver's licenses, something akin to REAL ID but currently doesn't exactly match the requirements of REAL ID. Twelve states have met 15 of 18 benchmarks, and another 12 states are falling short of that.

In addition, you have 13 states who have laws on the books saying they will not comply. You have another three who are saying we won't comply unless certain conditions are met, and often that goes to funding.

Of the five electronic databases necessary to really make REAL ID click, only two are nationally deployed and operational and being used by states. That is SAVE with regard to immigration status, and SSOLV with regard to Social Security. Of the other three, the passport system I believe may come online this year. EVVER, the Vital Records states, are joining and participating in digitizing their records, but that will not be fully implemented by the states

for some time, and there is not one DMV currently signed up to use EVVER. As a matter of fact, the pilot program for the DMVs expired last year.

And then the final one, the state-to-state driver's license system, which has taken time to satisfy the governance, the privacy, and how it will work between states, the implementation to get it to an operational system starts in 2015. It won't be fully ready, from the stats I have seen, until possibly as late as 2023. Yet those are the systems you really need to make this work from an electronic standpoint and get this working.

So where do we go from here? States need that clear guidance. For those numbers, those state numbers to become 100 percent, states need to be able to evaluate where they are and what the requirements are from DHS. We have heard and we look forward to additional guidance from the Department of Homeland Security to see exactly where states stand and whether or not January 15th, 2013 can be met. If it can't be met, it is probably not at the states' hands. It is because this was a bridge too far to begin with.

One of the reasons why governors have always been constructive partners is because driver's licenses have traditionally been the responsibility of the states. One of the reasons this has taken so long is because I believe the Federal Government found out how complicated this process is, how hard it is to validate those source documents, and how hard it is to check everything on those cards.

That being said, the states have made great strides. Getting the guidance out, being able to determine where we are, and then finding out what it is going to take to fill those gaps, including funding, I think will be critical to finally meeting the objectives of REAL ID, objectives that are shared by all governors, this Congress, and the Administration. Thank you.

[The prepared statement of Mr. Quam follows:]

Prepared Statement of David Quam, Director, Federal Relations, National Governors Association

Chairman Sensenbrenner, Ranking Member Scott, distinguished members of the committee; my name is David Quam, Director of Federal Relations for the National Governors Association (NGA). I appreciate the opportunity to appear before you today to discuss the issues surrounding state implementation of REAL ID.

OVERVIEW:

Governors have always been committed to providing their citizens with drivers' licenses that are accurate and secure. In fact, during multiple discussions among governors regarding REAL ID, it was clear that all governors share common principles regarding licenses and state identification:

- Licenses and identification cards should accurately reflect the identity of their owner;
- The systems that produce the cards and the cards themselves must be secure;
- Information received about individuals should be protected to ensure their privacy; and
- Services and products must be provided in a cost-effective manner that maximizes value for taxpayers without diminishing the security or integrity of the license.

It is through this lens that governors have viewed federal efforts to regulate state licenses, such as REAL ID. While governors believe that the objectives of REAL ID are laudable, they have found that the law represents an unworkable and unfunded

mandate that—without continued flexibility in its implementation—will fail to make us more secure.

BACKGROUND:

Congress passed the REAL ID Act (REAL ID) as part of the Emergency Supplemental Appropriations for Defense, the Global War on Terror and Tsunami Relief Act (P.L. 109–13). The law replaced section 7212 of the Intelligence Reform Act (P.L. 108–458), which established a negotiated rulemaking to determine national standards for state driver's licenses and identification cards (DL/IDs). NGA supported the compromise contained in section 7212 because it allowed stakeholders, including governors, to participate in the process of reforming what traditionally has been a state function.

Although the negotiated rulemaking was already underway, REAL ID repealed the provision and replaced it with statutory standards, procedures and requirements that must be met if state-issued licenses and identification cards are to be accepted as valid identification by the federal government. REAL ID's mandates require alteration of long-standing state laws, regulations and practices governing the qualifications for and the production and issuance of licenses in every state. Complying with REAL ID's standards will require significant investments by states and the federal government and will test the resolve of citizens directly affected by changes to state systems.

More importantly, all of this must be done quickly. The next milestone for states is January 15, 2013. As of that date, a state must be "materially compliant" with the act, or individuals can no longer use its licenses or identification cards to board commercial aircraft.

Given its impact on states and individuals, governors worked closely with other state groups, including the National Conference of State Legislatures and the American Association of Motor Vehicle Administrators, to recommend a regulatory framework that could bridge the gap between state laws and practices and the unrealistic requirements of REAL ID. NGA commends the Department of Homeland Security (DHS) for its continued efforts to develop a workable regulatory system to implement the law.

Unfortunately, even after the final rule was released, major issues remained including a lack of funding for state implementation; privacy concerns regarding the collection and use of individuals' information; and uncertainty regarding the availability, development and cost of electronic databases. These concerns ultimately helped propel 16 states to pass laws prohibiting compliance with REAL ID; laws that remain on the books today.

DEVELOPING A SOLUTION:

Given states' ongoing concerns, and the looming deadline for material compliance, governors asked NGA to work with state experts to develop recommendations to improve REAL ID based on the following principles:

1. Fulfill the 9/11 Commission recommendation for the "federal government to set standards for sources of identification;"
2. Facilitate and encourage participation by all jurisdictions;
3. Enhance the security and integrity of all licenses and ID cards while retaining state flexibility to innovate; and
4. Address critical privacy concerns and reduce unnecessary costs.

NGA's work culminated in the following recommendations:

- **Provide funds necessary for states to comply with federal requirements.** The projected costs of complying with the act far outweigh existing sources of funding. To the extent federal requirements result in increased costs for states, the federal government should fund the cost of complying with the law.
- **Allow for date-forward implementation.** To comply with the act, states should only be required to issue compliant DL/IDs beginning on a certain date. All DL/IDs issued after that date would comply with the federal law, but individuals would not be required to obtain a new DL/ID until their existing DL/ID expires. This provision would not apply to non-federally compliant DL/IDs issued by a state.
- **Limit required electronic verification of documents.** The final rule identifies five systems states will be required to use to be compliant with the

law: Social Security On-Line Verification (SSOLV); Electronic Verification of Vital Events Records (EVVER); Systematic Alien Verification for Entitlements (SAVE); an all-drivers system run by states to ensure an applicant is not licensed in another state; and a system run by the U.S. Department of State to validate foreign passport information. Of these systems, only SSOLV and SAVE are nationally deployed and functioning. Because of uncertainty regarding how and whether the five electronic systems will work, how they will be integrated and how they will ensure the protection of data, their use should not be required by federal law or regulation. Rather, states should be permitted to use existing verification processes to comply with federal requirements.

- **Establish a unique symbol to indicate that a license or identification card complies with federal requirements.** States should retain the authority to issue DL/IDs that do not meet federal standards. In order to differentiate between DL/IDs that meet federal requirements and those that do not, DHS should work with states to designate a means to easily identify federally compliant DL/IDs.
- **Provide greater clarification and flexibility regarding physical security requirements.** Not all departments of motor vehicles issue DL/IDs through the same process; some use central issuance (CI), others use over-the-counter issuance (OTC) and some use a hybrid CI/OTC process. Therefore, DHS should allow states to use a combination of security features designed to protect the physical integrity of DL/IDs. Many states have processes in place to issue, maintain and protect DL/ID information. Federal law and accompanying regulations should provide flexibility in how states prevent tampering, counterfeiting or unauthorized duplication of DL/IDs for fraudulent purposes.
- **Establish minimum guidelines for the further protection of personally identifiable information.** DL/ID information is protected by federal and state Driver Privacy Protection Acts (collectively, DPPA). However, since DPPA was enacted well before Real ID, DHS should establish further minimum guidelines to address requirements to protect the security, confidentiality and integrity of personally identifiable information that could not have been contemplated at the time of DPPA enactment.
- **Establish a process to allow states greater flexibility in validating an applicant's identity under exceptional circumstances.** States should be permitted to establish a process to validate an applicant's identity in rare cases where the applicant is unable to present the documents specified in the act.
- **Recognize enhanced driver's licenses as being compliant with REAL ID.** Enhanced driver's licenses issued by states should be considered compliant with requirements for secure state DL/IDs.
- **Establish a demonstration program to evaluate electronic information sharing among states.** The hub system envisioned by DHS in the final REAL ID rule is a complex and potentially costly endeavor, and participation in the system should not be federally required. Instead, the federal government should facilitate a demonstration program among a few states to determine projected costs for such a system, the appropriate governance structure for administrative purposes and the appropriate security and privacy measures to protect individuals' personal information.
- **Provide access to federal electronic systems.** Access to any federal electronic systems that states are required to use to comply with the act should be provided free of charge, just as the E–Verify system is made available to employers without cost.

PROVIDING FOR ADDITIONAL SECURITY IN STATES' IDENTIFICATION ACT:

In 2009, NGA supported S. 1261, the "Providing for Additional Security in States' Identification Act," (PASS ID) because it is built largely on governors' recommendations for solving the problems inherent to REAL ID.

For example, to address the issue of cost, PASS ID would have eliminated fees associated with the use of existing federally run databases that states must use to issue DL/IDs. It would also have allowed states to innovate to meet security requirements and eliminated the requirement to use electronic verification systems that do not yet exist or are not nationally deployed. If implemented, these changes would

have combined to cut state costs of compliance from $3.9 billion to approximately $2 billion.

PASS ID also recognized that at the time only two of the electronic systems states must use under REAL ID existed and were nationally deployed: SAVE to verify immigration status and SSOLV to verify social security information.

Today little has changed; SAVE and SSOLV remain the only two systems available although an electronic system to verify passports should be fully operational later this year.

Work to develop an electronic database to share DL/IDs information among states is slow, with implementation of an operational state-to-state system not anticipated until 2015. A fully deployed and populated system will not be available to states until 2023.

Likewise, a national vital records database to check birth certificates remains unfunded and lacking for data. Specifically, the recent recession and lack of federal funds has prevented states from digitizing their records—a necessary step for making a national database a reality.

PASS ID recognized these shortcomings by not requiring states to use systems that do not exist. It also addressed privacy concerns by requiring procedures to prevent the unauthorized access to or sharing of information, as well as requiring public notice of privacy policies and the establishment of a redress process for individuals who believe their personal information should be amended in records systems.

Finally, PASS ID tied timelines for issuance and full implementation to the completion of final regulations. Although not a true date-forward implementation schedule as called for by NGA, when combined with other enhancements, PASS ID would have allowed states to begin issuing compliant licenses and IDs faster than called for by REAL ID.

CONCLUSION:

Since its passage, governors have consistently offered constructive recommendations for implementing REAL ID. Governors have encouraged DHS and Congress to "fix" the act by implementing statutory or regulatory changes to make REAL ID feasible and cost-effective. They also have called on the federal government to "fund" REAL ID by providing federal dollars to offset state expenditures for meeting new federal standards.

If Congress wants to see REAL ID implemented, it needs to encourage and support the implementation of regulations and guidelines that make compliance a possibility. DHS has worked closely with states to understand the complexities of the DL/ID process and provide rules that encourage better and more secure DL/IDs in a more cost-effective and realistic manner. More, however, needs to be done.

Security of our nation is not a partisan issue. Every governor is a security governor. Every governor is interested in making government work. Governors look forward to continuing efforts with Congress and DHS to find workable, cost-effective solutions that can increase the security and integrity of all state license and identification systems.

Mr. SENSENBRENNER. Thank you very much.

The Chair is going to clean up and ask questions last. So the gentleman from Virginia, Mr. Scott, is recognized.

Mr. SCOTT. Thank you, Mr. Chairman.

I guess, Mr. Williams, what ID is necessary to get a REAL ID? What does a person have to present in order to get identification?

Mr. WILLIAMS. Well, what an individual would need to do is present source documents, for example, such as a birth certificate, and if they have a Social Security number, they should present that Social Security card or another acceptable document with the Social Security number so that number can be verified.

If they are in the country, for example, with immigration papers, then they certainly need to present their immigration document to be verified.

Mr. SCOTT. Let me just—for a citizen just trying to get an ID——

Mr. WILLIAMS. For a U.S. citizen?

Mr. SCOTT. Yes.

Mr. WILLIAMS. A birth certificate and Social Security card.

Mr. SCOTT. Now, what do you need to do to get a birth certificate?

Mr. WILLIAMS. To get a birth certificate, different states have different processes in regards to how you get it and who is authorized to get a birth certificate. But in many cases, I think you would have to go to your vital records agency within that state to request a birth certificate. And again, that is the general term. Different states have different processes.

Mr. SCOTT. And again, what do you have to present to get the birth certificate?

Mr. WILLIAMS. Each state I think has a different process for it.

Mr. SCOTT. Could a terrorist show up and get a birth certificate, my birth certificate?

Mr. WILLIAMS. That is a question I couldn't answer. I don't participate in the vital records agency processes.

Mr. SCOTT. I don't know where my Social Security card is. I know my number, but I wouldn't have a clue as to where the actual card is.

Mr. WILLIAMS. If you don't have your Social Security card, there are other documents that you can use with that Social Security number.

Mr. SCOTT. Okay.

Mr. WILLIAMS. For example, if you are employed and you have a W-2——

Mr. SCOTT. If two people were wandering around using the same birth certificate or the same Social Security number, is there something in the system that would expose that?

Mr. WILLIAMS. Well, Social Security, the agency has the capability to identify——

Mr. SCOTT. A lot of people sell Social Security numbers, those that would actually check when you go through the process, as a valid Social Security number. How do you know that the person before you is the one with that Social Security number?

Mr. WILLIAMS. Again, that would be a process of checking with the Social Security Administration and using their processes.

Mr. SCOTT. REAL ID doesn't solve this.

Mr. WILLIAMS. No, REAL ID doesn't govern that process.

Mr. SCOTT. Mr. Heyman, is possession of a fake ID a crime?

Mr. HEYMAN. I believe it is.

Mr. SCOTT. You believe it is?

Mr. HEYMAN. I don't know.

Mr. SCOTT. You don't know.

Mr. HEYMAN. Use of it is a crime.

Mr. SCOTT. Use of it. But, I mean, if you just ran across somebody and they had three or four different IDs in their pocket, would that be a—you don't know if that is a crime or not? Okay.

Mr. Williams, you indicated exposure of employee fraud. If you have a DMV clerk somewhere in some rural area just making money by selling fake IDs, would these IDs be as good-looking as other IDs?

Mr. WILLIAMS. The most valuable ID that you can actually get is working with an internal person to produce one based upon the internal processes of that particular state's DMV. The cost for that

process, to show you how realistic it is, for example in New York, they were selling fake IDs for as much as $10,000 per copy. In the State of, for example, Maryland, a fake ID produced internally could render as much as anywhere from $2,500 to $3,000; California, anywhere from about $5,000——

Mr. SCOTT. Well, if you have bribed a DMV official, will the ID be—would anybody be able to ascertain that this is a fake ID?

Mr. WILLIAMS. If the ID is produced internally, it will be exactly the same as any other ID. That is the value of finding someone who works inside, and that is what REAL ID seeks to prevent.

Mr. SCOTT. How does it prevent internal fraud?

Mr. WILLIAMS. By coming up with a number of internal processes that the DMV must actually utilize, for example, to include background checks of its employees, but also internal processes to ensure that, for example, one person does not have the authority to actually produce a driver's license from start to finish, and then other internal processes like, for example, making sure that you have a photo of the individual who sought a driver's license through application so you can actually check internally to see whether or not that photo shows up on any other driver's license with a different name and Social Security number.

Mr. SCOTT. Is that check actually done anywhere?

Mr. WILLIAMS. That check is actually done by a number of DMVs today. With the advent of REAL ID, that number of internal checks has gone up significantly.

Mr. SCOTT. If I can just follow up on this with one question?

Mr. SENSENBRENNER. Without objection, the gentleman has one more question.

Mr. SCOTT. If two people are using the same photo, that would be exposed?

Mr. WILLIAMS. If two people were using the same photo at the same DMV, DMVs have——

Mr. SCOTT. The DMVs, one is in Connecticut and one is in Virginia.

Mr. WILLIAMS. Well, if they were in different states and those states did not have a process where they actually shared photos, then that would be more difficult. But in the same state, a number of states have same-day processes where they take your picture and then run it through the database and check with all other photos in their database to see whether you are the person you claim to be. And then on a 24-hour basis, they run it through their entire system to process to see whether or not you have a, quote unquote, face that is recognized in their database, and then what they have is control investigators. Once they ascertain that you may have a photo already in their database, the investigator is actually used to pursue to determine whether or not you are an exact match or if you are a similar match but not necessarily the exact same person.

So a number of processes are in place to prevent the same photos with different IDs inside the state level. States have cooperative sharing relationships where they are actually starting to share some of their photos across state lines to ensure that you don't have, for example, a picture ID in the State of North Carolina, but also in the State of South Carolina.

Mr. SENSENBRENNER. I guess all this was done because of REAL ID.

The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thanks, Chairman Sensenbrenner.

Let's use this time to focus on the two issues that have been so well raised in this discussion, and I want to thank attorney Stewart Baker for his emphasis on the privacy issue. Let's talk about how we fund and how we guard for privacy. Remember now that we may be meeting with the Secretary Napolitano on this subject, and we want to use these minutes to get your best advice as to how we deal with her, with the Chairman, with these two issues.

Let's start off with you, David Quam, and then let's everybody just chime in when you want to.

Mr. QUAM. Thank you, sir. I think the emphasis with the Secretary has really got to be first and foremost with the guidance that needs to come out so states know exactly where they are. So knowing those rules so states can evaluate where we are today and where states need to be by January 15th is critical. I think that guidance is pending and will come out very shortly.

With regard to privacy, governors have always been concerned with governance of these systems. It is how the systems work, but how are they governed? How is individual information being protected, and how can it be corrected if there is a mistake, to make sure there aren't false-positives?

So, very large privacy concerns that need to be worked out. That is why some of those systems are going to take some time to bring online, and privacy guidance is critical, and hopefully it is going to be part of this next guidance.

And then finally, with regard to funding, states have long said this is an expensive proposition. If it is a mandate from the Federal Government, it should be paid for by the Federal Government. One simple example that we have called for, if there is a requirement to use Federal systems, then those Federal systems should be free to the states, much like e-Verify is for a lot of businesses. The Federal Government has the databases, let us use that. It is part of the problem we have had with vital records where there is a fee that has to be charged every time. In the fiscal condition of states, that can be very problematic. But with some funding for states, I think you can find that states can more easily come on board.

Mr. SCOTT. Attorney Stewart Baker.

Mr. BAKER. On the privacy issue, to my mind the biggest privacy issue in this area is not having a good ID. I don't understand what privacy interest is served by having a bad ID. The real privacy concern is the risk that your identity will be stolen and someone will use a fake ID to pretend to be you.

The Department has lots of information about people who are engaged in that kind of identity fraud, and there needs to be better coordination with the states so that they don't continue to issue driver's licenses to people using bad Social Security numbers and so they can reinvestigate people who may have used bad Social Security numbers to get their cards in the first place.

So that would be a privacy issue that I think would be very useful to address. I do think the Department has done a good job of

coming up with some additional privacy standards that they think should be met by states to protect data, and that is a good thing.

On the question of unfunded mandate, I think that is—I don't agree with it, and the problem with that is the argument that somehow the Federal Government should make free the SSOLV and SAVE programs that allow you to use the government's records to check Social Security numbers and the like. Those cost pennies, maybe 20 cents. The states, on the other hand, have put in place EVVER, in which they propose to charge $2 a check, the income of which they are going to keep to use for——

Mr. CONYERS. Do you prefer the state solution?

Mr. BAKER. This is the state electronic event verification, essentially the birth record database. The current prices for that are $2 because the state vital records offices want to make about $1 every time they provide this information. For the states to say we want to charge you dollars and we want you to forgive the pennies that we are paying is inconsistent, I think.

Mr. CONYERS. Let me get to Darrell Williams.

Mr. WILLIAMS. There are only three issues we are talking about: privacy, cost, and a recommendation for DHS. On privacy, most of the data that we are talking about already exists in various state DMV databases. States use what they call—this is actually run by the Department of Transportation—the CDLIS system, and that CDLIS, which is a commercial driver's license information system, actually contains the name, date of birth, and driver's license information for virtually all drivers already, because whenever anyone applies for a CDL, a commercial driver's license, they are run through the CDLIS system to determine whether or not they have a commercial driver's license somewhere else. So the data that we are pretty much talking about in regards to privacy concerns, it already exists in the database.

The second issue, we talked about cost, and actually I will piggyback on an example that you gave in regards to Mark Sanford. Of course, now, Mark Sanford did write a letter. Actually, he wrote a couple of letters to DHS that went to Secretary Chertoff, but also to Napolitano, where he expressed concern about REAL ID and its cost. However, in that same letter Mark Sanford said that South Carolina, at the time of his writing, currently met about 90 percent of the REAL ID requirements. So if he was concerned about cost, he is 90 percent there. There is only a 10 percent delta, and the delta wasn't going to be overly substantial at the time when I actually read his letter and talked with Marcia Adams, who is the South Carolina DMV Director in that timeframe to determine exactly where South Carolina was. So the cost delta using that example was not going to be that great.

The last item in regards to a recommendation for REAL ID implementation, REAL ID is a program, and REAL ID is managed pretty much out of a program office. I know because I started it. However, the enforcement part about REAL ID today is that program and that program office remains in a policy environment, which is the exact wrong place for a program to be.

The skill sets are not there. The program management skills are not there. The engineering skills are not there. So if you are designing and developing an information-based system, policy is the

exact wrong environment to be in for a program to thrive and flourish as we look at going forward.

Mr. SENSENBRENNER. Without objection, the gentleman from Michigan will be given an additional minute.

Mr. CONYERS. I thought it was 2 minutes.

Mr. SENSENBRENNER. No. I said you were already 2 minutes over.

Mr. CONYERS. Oh. Thank you very much. Mr. Heyman, please.

Mr. HEYMAN. Thank you, Congressman. Thank you. Let me just talk on those three points that you are interested in.

First, in terms of the privacy, the REAL ID Act did not contemplate or stipulate privacy requirements, but we did put in the regulation privacy requirements on the states. There are standards for data protection, particularly on the network. There will be encryption standards, and as Mr. Williams mentioned, the networks are built on private networks that already exist with privacy protections.

We are moving forward with guidance, as the states have asked for. That guidance will, I believe, help provide clarity for helping on compliance questions by providing comparable programs that had not possibly been contemplated.

And then lastly on the funding question, funding this year, the Secretary did sign out in February 2012 new FEMA grant guidance to state administrative agencies to help address and to be used for funding driver's license security grant programs.

Mr. CONYERS. Thank you.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentleman from Colorado, Mr. Polis.

Mr. POLIS. Thank you.

My first question is for Mr. Heyman. I am concerned that there are several classes of legal immigrants who would not be eligible for a license under this law. Some of those include non-immigrant visas such as victims of trafficking, immigrants who have been paroled into the U.S. for humanitarian reasons, battered immigrants who are awaiting actions or on petitions filed with U.S. CIS. These are some of the most vulnerable legal immigrants in our country.

Does the law need to be fixed so these people can get a license, or is there some procedure under this law where these groups of legal immigrants would be able to get licenses?

Mr. HEYMAN. Well, under the REAL ID Act and regulations, lawful presence is assessed and determined, but the actual determination of who to issue a state driver's license for operating a vehicle but perhaps not REAL ID-compliant is left to the state. So that decision is a state decision.

Mr. POLIS. But the issue is whether the ID would be useful for Federal purposes, and I think it is in many ways a backdoor Federal takeover of the licensing requirement for the states. Do you anticipate that the states will have two sets of licensing requirements, one REAL ID-compliant and one not? Is that what you are contemplating?

Mr. HEYMAN. We are not—we are contemplating that if a driver's license is to be used for Federal purposes, it must be REAL ID-compliant.

Mr. POLIS. As far as you know, are any of the states maintaining two separate types of driver's license, one REAL ID-compliant and one non?

Mr. HEYMAN. We don't have an assessment at this point, as you know, because the compliance deadline has not been met yet. We do not have visibility into what all states are contemplating.

Mr. POLIS. Have any states brought that up to the agency, that they are considering doing a two-ID approach?

Mr. HEYMAN. I am not aware of that.

Mr. POLIS. Okay. Again, so the concern is, again under the REAL ID requirements, which are being heavily pushed to the states, it is my understanding that a victim of trafficking or a legal immigrant who has been paroled in the U.S. for humanitarian reasons or a battered immigrant who is awaiting actions on a petition filed under U.S. CIS, at least those three categories of immigrants it is my understanding are not able to get REAL ID-compliant driver's licenses. Is that consistent with your understanding?

Mr. HEYMAN. An individual must be able, must present, must be lawfully present in the United States to attain a driver's license. So if they are lawfully present, they will be, along with all the other requirements.

Mr. POLIS. Okay. Well, those are people who are lawfully present in the United States, but they are legal immigrants, not illegal immigrants. But it is my understanding that in some cases, because their cases are pending, they would be unable to get the REAL ID. But are you saying they would be able to get a REAL ID-compliant state ID?

Mr. HEYMAN. I am not aware of an exception to that. So if the Congressman would allow, we can get back to you on the record.

Mr. POLIS. We will be happy to get you some specifics.

Let me go to Mr. Baker. It is my understanding DHS postponed the REAL ID implementation under the Bush Administration, and I would like to ask what those reasons were for that postponement over those period of years.

Mr. BAKER. We concluded that the states, by and large, were not going to meet the deadline. It was a pretty demanding set of requirements. They had been fighting them. They had been hoping to delay the implementation. And we broke the implementation into two stages, material and full compliance, so that we could get the states to a place with about a 1-year extension where they were implementing most of REAL ID. So we gave them a relatively short extension to meet, I would say, 90 percent of the requirements, and in exchange for that we got their assurance that they were working diligently toward achieving the standards of REAL ID.

Mr. POLIS. Mr. Quam mentioned that the original was untenable and the flexibility was critical. I would like to ask Mr. Quam, is there sufficient flexibility in the current law, or do we need to go back and add additional flexibility to ensure that this can be implemented?

Mr. QUAM. It is quite possible that we need additional flexibility. Part of the reason for the delay was the first set of regs really was untenable. It was not going to provide the opportunity for states to truly implement the law. I think DHS did a very good job of listening to the states. I have to congratulate the Department, both Ad-

ministrations, for listening to the states and realizing how complex this was in making changes.

I think this next set of guidance is going to be critical for states to evaluate where we are and what other flexibilities need to be put in. Again, with regard to some of the databases that are necessary, they are just not there. If they are not there, states cannot be required to meet a compliance standard that is impossible to meet. So that flexibility has to be there to get states to move forward. States are moving forward. They are doing the best they can with the rules as we have them.

Mr. POLIS. I just want to ask for 30 seconds?

Mr. SENSENBRENNER. Without objection.

Mr. POLIS. And the final question, Mr. Quam. So again, without additional flexibility, do you believe that there would have to be additional postponing of the hard deadline for the REAL ID Act to go into effect?

Mr. QUAM. Until we see the guidelines, it is impossible to say what is going to be necessary for the states. States do have to make progress in order to meet the rules as they stand today. I think that guidance and an evaluation by the states is going to be critical to determine that question.

Mr. POLIS. Thank you, and I yield back.

Mr. SENSENBRENNER. The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

Under the REAL ID Act, an individual's address has to be on the face of the card, but many individuals ranging from law enforcement and judges to victims of domestic violence may be put at risk due to this requirement. Mr. Heyman, there are many domestic violence victims who don't want their address on the ID card, and there are many victims of domestic violence. One in four women will experience domestic violence in her lifetime.

What is DHS doing to address this issue, and has there been any study of the effect of these provisions on survivors of domestic violence, sexual assault, or stalking?

Mr. HEYMAN. There are provisions for alternative ways for identification, the specifics of which I would actually turn to my colleague here, who used to work for me, who actually helped implement them.

Mr. WILLIAMS. The rule as written today does allow for individuals that are victims of domestic violence not to have their home addresses displayed, for law enforcement and judges as well.

Ms. CHU. So there are allowances for that?

Mr. WILLIAMS. Yes.

Ms. CHU. Let me ask about another issue. Actually, Mr. Williams, I would like to address this to you, and that has to do with the fact that, of course, there are more stringent requirements for the REAL ID Act, and yet at the same time there is another thing going on, which is that at least 34 states have introduced legislation just this last year that would require voters to provide a photo ID when they go to vote. At least 12 states have introduced legislation that would require proof of citizenship such as a birth certificate to register to vote.

To what extent—and Mr. Heyman, too—to what extent has the Department been monitoring the recent attempts to enforce these ID requirements and its impact on voting?

Mr. WILLIAMS. For that, I would have to really refer back to the Secretary Heyman in regards to what DHS is doing to monitor.

Mr. HEYMAN. Well, we are aware of those provisions. They are not material to the compliance for REAL ID, but we are certainly paying attention to that.

Ms. CHU. Let me ask about the 25 states that have, through statute or legislative resolution, rejected their intent to comply with the Act. I know there has been some dialogue and so forth, but what conversations has DHS had with governors and state legislatures to address their concerns with the Act? And also, if REAL ID is implemented by 2013, what implications will it have for citizens from these states if there are still those that reject the REAL ID Act? Will citizens from these states no longer be able to board a plane? What implications are there for their everyday life, Mr. Williams and Mr. Heyman?

Mr. HEYMAN. Well, let me just say that if you look at all states and all territories to include those that have acts against REAL ID, all of them have made progress on driver's license security. In fact, if you look at the material compliance, the 18 benchmarks for material compliance, 83 percent of those with benchmarks, states have committed to meeting or are already meeting 83 percent of those.

What that reflects is that while the actual compliance with the specific Act may have been rejected by some states, they are continuing to make progress on the actual underlying security standards.

Mr. WILLIAMS. I would say one of the other advantages that citizens of those states would have is REAL ID is only required when an individual goes to the airport and is asked to produce a form of ID. If that person chooses to produce a driver's license as a form of ID is where the REAL ID requirement would come in. There are other forms of ID a person could actually produce, and that could be very well accepted by the TSA individuals at the airport. Or, for example, a person could very well have no form of ID and still be allowed to get on an airplane.

So they do have alternatives and options if, by chance, you are addressing the issue as to, when they go to the airport, whether or not they would be allowed to actually board a commercial airline. So, yes, there are options available for them in any of those states.

Ms. CHU. And the other forms of ID for boarding a plane would be?

Mr. WILLIAMS. Please?

Ms. CHU. The other forms of ID you said would be acceptable for boarding a plane?

Mr. WILLIAMS. Well, there's a TSA list of items that they accept, I guess on the TSA website, I believe, in regards to what are acceptable forms of identification other than a driver's license.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

The gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, thank you very much, and thank you for holding this hearing that reviews what I think is a stalled law ready for burial. I believe the REAL ID Act was imple-

mented in 2005, and it seems as if implementation has completely stalled, and there seems to be resistance to the REAL ID implementation in the states, and it is guaranteed that the statute seemingly will never be implemented as it is currently drafted.

It was passed as a rider to a bill funding the military expenditures and tsunami relief, so it obviously slipped under the radar screen. But it gives states 3 years to bring their driver's license into compliance with the Act's requirements, common licensing standards national database, et cetera. It is now 2012. That is 7 years. The REAL ID has faced opposition from civil rights and civil liberties, but I think the real question is the lack of sufficient protections.

We are now in the midst of another rage of what we call voter ID laws in 40 states, all being confronted with the real issue of denying someone a birthright, a citizen's right to vote. They have been previously able to identify themselves, have a voter registration card.

So I want to ask the representative of the National Governors Association. I have never known the National Governors Association to not be quite prompt, and not only prompt but conversant and ready to adhere to Federal laws, but I am respectful of the fact of the different requirements of each state. Tell me why this has been so difficult and what I perceive to be opposition to implementing a law passed in 2005. And I might just put on the record that there are those opponents that come from all political perspectives who are dealing with questions of civil liberties and civil rights. But let me hear from the representative of the National Governors Association, please.

Mr. QUAM. I greatly appreciate the question. I think a lot of the problem initially was a misunderstanding of how driver's license systems work, and there was an education process that had to go on between the time of the passage of the bill and ultimately the regulations that came out, and then the regulations that were rewritten. As everybody learned how difficult the processes are, the fact that the states have been doing this for over 100 years and not the Federal Government, and that combining rules for the Nation when you have each state doing their own is a difficult process.

And so what happened is that governors really tried to be constructive partners to find a solution. One of our key calls was fix and fund REAL ID early on. Later it became let's take the strengths of REAL ID and get rid of its problems. That became the PASS ID Act that was introduced, at least in the Senate.

You still see states today trying to improve and meeting some of these benchmarks, the integrity of their licenses, because every governor is a security governor. They want their driver's license to be secure and safe. But very real problems were raised on both sides of the aisle with regard to privacy, with regard to the reach of the Federal Government into state actions, and then ultimately how do you get this done, how do you find a solution that makes the most sense.

The original compromise for a negotiated rulemaking was something that governors and states were willing to participate in and were active participants. I think if that had been allowed to go forward, we may be further than we are today. But like I said, there

was a partnership formed between governors, between states, the Department of Homeland Security, and even many Members of Congress to try to find a way forward. You have seen a lot of progress, but there are still a lot of objections, and there are 16 states who still have a law on the books today saying we will not comply.

It is a problem when one-fourth of the states say we are not participating in a national system. It is hard to have a national system when one out of every four isn't participating.

Ms. JACKSON LEE. Let me thank you for that explanation. I know that, as a Member of the Homeland Security Committee, I will be probing this independently, and I am not going to probe Mr. Heyman at this time. I think the record is going to be very clear in this hearing. It is not functioning. It is not working. I think the privacy issues are severe, and I think that this adds to the opposition to this massive plague of voter ID laws. It just compounds fears.

I just came out of a hearing dealing with Hezbollah and homeland concerns on Hezbollah's presence on the homeland. Yes, that is where we need to be focusing. And, yes, we need to be acknowledging that 9/11, tragic as it was, that our message was that we are not going to allow terrorists to cause ourselves to undermine our basic civil liberties and privacy.

So I just want to yield back at this time and say that my concern remains on this REAL ID law, and I believe it is not effective at this time. I yield back.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

It seems from this hearing that because of the REAL ID law, there have been significant improvements in the security of state IDs, even in the states that rejected the REAL ID law. And Mr. Quam I notice is nodding his head, and so we will put that in the record.

I think one of the ways to get the ball over the goal on this—and I realize as the author of the bill that this is a complicated bill—is, first of all, states need guidance; and secondly, the DHS has to show that it is serious that there is a deadline.

So, Mr. Heyman, let me ask you, when are the states going to get some guidance, better guidance?

Mr. HEYMAN. Guidance is in OMB now for clearance. It should be forthcoming in the next couple of weeks.

Mr. SENSENBRENNER. That is good. Now, during an oversight hearing that this committee had last November, Secretary Napolitano refused to say whether or not the DHS would hold firm to the January 15th, 2013 deadline. Is DHS going to extend the deadline again?

Mr. HEYMAN. We have no plans to extend the deadline.

Mr. SENSENBRENNER. That is good. Now, Mr. Heyman, in your testimony you state that REAL ID regulation, as opposed to the law, provides DHS with the ability to recognize comparable programs in states and territories that issue driver's license and ID cards consistent with the minimum requirements of the regulation. But the REAL ID Act does not differentiate between requirements that are mandatory and those that are discretionary. Please inform

the committee which part of the REAL ID Act authorizes DHS to make that distinction.

Mr. HEYMAN. Congressman, what we are looking to do here is to take the brilliant invention of states which allowed for innovation in a democratic society and to capture that, in effect, such that one state that may have thought of a solution for implementation of the regs that we had not originally contemplated but was consistent with the regs could be identified and shared with others. That is the purpose of putting forward comparable programs.

Mr. SENSENBRENNER. Well, in my high school civics class, I learned in a democratic society that laws that are passed by a majority vote of the legislature and signed either by the President or the governor are the law. Now, has that basic constitutional principle penetrated DHS or not?

Mr. HEYMAN. The law is the law, Congressman, and the ways in which states can comply with that law, there may be comparable programs that, with technology or otherwise, that allow for consistent application of the law through state by state innovations.

Mr. SENSENBRENNER. Okay. Let's get back to the guidance. Why has the DHS waited so long to issue the guidance?

Mr. HEYMAN. The guidance has been in development over a period of probably a little over a year, and it is forthcoming now. I think it is timely. It will give states an opportunity to assess where they are in the compliance process, and for us to do the same.

Mr. SENSENBRENNER. Well, the law was signed in 2005 by former President Bush. Did it take DHS 6 years to start doing the guidance and now we are about ready to get to it?

Mr. HEYMAN. Well, the history of the implementation is that first the Department established a regulation and an implementation plan, and then it issued two other forms of guidance in 2009. In our dialogue, this is a partnership with the states, and in our dialogue with the states it has become clear that they have sought additional clarity, and we are therefore putting forward additional guidance.

Mr. SENSENBRENNER. Okay. Now, my final question is there has been a disconnect between DHS and the states, both in this Administration and in the Bush Administration on this subject. How many states has DHS visited or AAMVA meetings has DHS participated in with regard to the REAL ID Act?

Mr. HEYMAN. I believe we have traveled to 44 out of 56 states or territories, and I can't give you the number on AAMVA participation, but we regularly, perhaps even annually, participate in their national convention.

Mr. SENSENBRENNER. Okay. Well, thank you. I think that completes the record. I yield back the balance of my time.

Are there any further items that Mr. Scott wants to put into the record?

Mr. SCOTT. Well, Mr. Chairman, we have had statements from others that we would like into the record, if we could.

Mr. SENSENBRENNER. Without objection, both the majority and the minority may put additional statements into the record that are relevant and material to the purpose of this hearing or the testimony of the witnesses.

Hearing none, so ordered.

And without objection, this hearing is adjourned. I thank all of the witnesses for their testimony.

[Whereupon, at 11:17 a.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

before the
House Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

March 21, 2012

Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards

The American Civil Liberties Union (ACLU) writes today to oppose any additional efforts by Congress or the Department of Homeland Security (DHS) to force states to comply with the Real ID Act of 2005. We believe any such actions would not only harm individual liberty, but also waste scare government resources.

Implementation of the Real ID Act is completely stalled. Resistance to Real ID implementation in the states has guaranteed that the statute will never be implemented as it is currently drafted. Compliance with the Real ID Act is statutorily barred in 15 states and the law has been rejected by statute or resolution in at least 25 states. This state rebellion has caused DHS to postpone implementation of the statute repeatedly.

And DHS has no effective tools to induce state compliance in the future. Under Real ID, the only remedy DHS can impose on non-compliant states is to deny the citizens of those states the right to use their drivers' licenses to board airplanes or enter federal facilities. Because DHS has rightly recognized that it cannot possibly paralyze the air transportation system or deny tens of millions of Americans the right to fly, it has chosen to postpone implementation of the Act repeatedly. Moreover, Congress has provided only a small fraction of the funding that would be necessary to comply with the law. DHS should recognize these facts and end all administrative measures aimed at compliance. Ultimately Congress should repeal Real ID.

The ACLU is America's oldest and largest civil liberties organization dedicated to the principles of liberty and justice set forth in the U. S. Constitution. On behalf of more than half a million members, countless additional supporters and activists, and 53 affiliates nationwide, we advocate against unnecessary government intrusion into the lives of Americans and undue burdens on their privacy rights.

Background

The Real ID Act of 2005 was passed as a rider to a bill funding military expenditures and tsunami relief.[1] The law gave states three years to bring their drivers' licenses into compliance with the Act's requirements including common licensing standards and a national database of drivers' license information.

Instead of compliance, Real ID faced widespread opposition. Groups from across the political spectrum opposed it. Civil rights and civil liberties groups worried that the Act lacked sufficient protections and might increase racial discrimination. Defenders of religious freedom described its negative impact on the Amish and other religious denominations. Consumer groups feared it would result in an expansive and cumbersome new bureaucracy.

Others rejected Real ID as a national ID. Many groups, including the ACLU, believed it would facilitate tracking of data on individuals and bring government into the very center of every citizen's life. It would be a de facto government permission slip needed by everyone in order to travel. As happened with Social Security cards decades ago, use of such ID cards

[1] Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Public Law 109-13, 119 Stat. 231, 302 (May 11, 2005) (codified at 49 U.S.C. 30301 note).

would then quickly spread and be used for other purposes – from work to voting to gun ownership.

Many states rejected Real ID because of its high cost – initially estimated by DHS at $23 billion. States were concerned that the Act would force them to change their entire licensing issuance process to conform to a one-size-fits-all federal mandate. At the same time the states were also making great strides in improving drivers' license security and were rightly concerned that Real ID would interfere with or overturn many of these efforts. Since Real ID's passage Congress has appropriated only $200 million for compliance with the statute.[2]

State Statutes and DHS Extensions

Twenty five states, either through a statute or legislative resolution, rejected the Act or said they would not comply with Real ID.[3] Fifteen states have laws prohibiting compliance with Real ID. Many of these provisions are complete bars on any participation by the state in the program. Other states have funding and security requirements for participation that the federal government will almost certainly never meet.

The 15 states prohibiting compliance are:

1. Alaska – ALASKA STAT. § 44.99.040 (2007-2008) (A state agency may not expend funds solely for the purpose of implementing or aiding in the implementation of the requirements of the federal Real ID Act of 2005 (P.L. 109-13, Division B)).

2. Arizona – ARIZ. REV. STAT. ANN. § 28-336 (2008) (This state shall not participate in the implementation of the REAL ID act of 2005 (P.L. 109-13, Division B; 119 Stat. 302). The department shall not implement the REAL ID act of 2005 and shall report to the governor and the legislature any attempt by agencies or agents of the United States DEPARTMENT of homeland security to secure the implementation of the REAL ID act of 2005 through the operations of the United States department of homeland security.)

3. **Georgia** – GA. CODE ANN. § 40-5-4.1 (2010) (The Governor of the State of Georgia, or his or her designee, is authorized to delay compliance with certain provisions of the federal Real ID Act, H.R. 1268, P.L. 109-13, enacted by Congress in 2005, until it is expressly guaranteed by the Department of Homeland Security, through adequately defined safeguards, that implementation of the Real ID Act will not compromise the economic privacy or biological sanctity of any citizen or resident of the State of Georgia.)

---

[2] Shawn Zeller, *States Rev Up For Real ID*, CQ, Feb. 13 2012.

[3] The states are Alaska, Arizona, Arkansas, Colorado, Georgia, Hawaii, Idaho, Illinois, Louisiana, Maine, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, North Dakota, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Virginia and Washington.

4. **Idaho -** IDAHO CODE ANN. § 40-322 (2008) (The legislature hereby declares that the state of Idaho shall not participate in the implementation of the REAL ID act of 2005. The Idaho transportation board and the Idaho transportation department, including the motor vehicles division of the Idaho transportation department are directed not to implement the provisions of the REAL ID act of 2005.)

5. **Louisiana** – LA. REV. STAT. ANN. § 402 NOTE (2008) (The Legislature of Louisiana does hereby direct the Department of Public Safety and Corrections, including the office of motor vehicles, not to implement the provisions of the REAL ID Act and to report to the governor any attempt by agencies or agents of the United States Department of Homeland Security to secure the implementation of the REAL ID Act through the operations of that division and department.)

6. **Maine** - ME. REV. STAT. ANN. tit. 29-A, § 1411 (2007) (The State may not participate in the federal REAL ID Act of 2005, enacted as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Public Law 109-13. The Secretary of State may not amend the procedures for applying for a driver's license or nondriver identification card under this chapter in a manner designed to conform to the federal REAL ID Act of 2005.)

7. **Minnesota** – 2009 MINN. LAWS CHAPT 92 (The commissioner of public safety is prohibited from taking any action to implement or to plan for the implementation by this state of those sections of Public Law 109-13 known as the Real ID Act.)

8. **Missouri** – MO. REV. STAT.§ 302.183 (2009) (The Department of Revenue is prohibited from: (1) Amending any procedures for applying for a driver's license or identification card in order to comply with the standards of the federal Real ID Act of 2005; (2) Expanding motor vehicle records data it shares with other states, the federal government, or other agencies or providing data to any additional states or state or federal agency unless authorized by statute; or (3) Collecting, obtaining, or retaining any data in connection with activities related to compliance with the act.)

9. **Montana** – MONT. CODE ANN. § 61.5.1 (2007) (The state of Montana will not participate in the implementation of the REAL ID Act of 2005. The department, including the motor vehicle division of the department, is directed not to implement the provisions of the REAL ID Act of 2005 and to report to the governor any attempt by agencies or agents of the U.S. department of homeland security to secure the implementation of the REAL ID Act of 2005 through the operations of that division and department.)

10. **New Hampshire** – ([T]he state of New Hampshire shall not participate in any driver's license program pursuant to the Real ID Act of 2005 or in any national identification card system that may follow therefrom. ... The department of safety shall not amend procedures for applying for a driver's license under RSA 263 or an identification card under RSA 260:21 in order to comply with the goals or standards set forth in the Real ID Act of 2005, or in any rules or regulations promulgated

thereunder, or in any requirements adopted by the American Association of Motor Vehicle Administrators for such purposes. ... The department of safety shall not expand the motor vehicle records data it shares with other states, the federal government, or other agencies, or provide motor vehicle records data to any additional states or state or federal agencies unless authorized by statute.)

11. **Oklahoma** – OKLA. STAT. ANN, tit. 47, § 6-110.3 (2007) (The State of Oklahoma shall not participate in the implementation of the REAL ID Act of 2005. The Department of Public Safety is hereby directed not to implement the provisions of the REAL ID Act of 2005 and to report to the Governor and the Legislature any attempt by agencies or agents of the United States Department of Homeland Security to secure the implementation of the REAL ID Act of 2005 through the operations of that or any other state department. ... No department or agency of the state charged with motor vehicle registration or operation, the issuance or renewal of driver licenses, or the issuance or renewal of any identification cards shall collect, obtain, or retain any data in connection with activities related to complying with the REAL ID Act of 2005.)

12. **Oregon** – 2009 Or. Laws Chapt 432 (A state agency or program may not expend funds to implement the Real ID Act of 2005, P.L. 109-13, unless: (1) Federal funds are received by this state and allocated in amounts sufficient to cover the estimated costs to this state of implementing the Real ID Act of 2005; and...Sufficient measures to protect the privacy of individuals; and ... Sufficient safeguards against unauthorized disclosure or use of an individual's personal identifying information by department personnel or any contractor, agency or other person who may have access to the database, records facility or computer system.)

13. **South Carolina** – S.C. CODE ANN. § 56.1.85 (The State shall not participate in the implementation of the federal REAL ID Act.)

14. **Virginia** – VA CODE ANN. § 2.2-614.2 (2005) (Provides that, with the exception of identification cards issued to employees of the Department of State Police and certain other law enforcement officers, the Commonwealth will not comply with any provision of the federal REAL ID Act that it determines would compromise the economic privacy, biometric data, or biometric samples of any resident of the Commonwealth)

15. **Washington** WASH. REV. CODE § 43.41.390 (A state agency or program may not expend funds to implement or comply with the REAL ID Act of 2005, P.L. 109-13, unless ... federal funds are received by the state of Washington ... in amounts sufficient to cover the costs of the state implementing or complying with the REAL ID Act of 2005... the department of licensing shall certify that the driver's license, identicard, database, records facility, computer system, and the department's personnel screening and training procedures: (1) Include all reasonable security measures to protect the privacy of Washington state residents; (2) include all reasonable safeguards to protect against unauthorized disclosure of data; and (3) do not place unreasonable costs or recordkeeping burdens.)

As mandated by these fifteen statutes, these states will never comply with Real ID. It would be illegal for state officials to do so and has thereby created an impossible situation for DHS.

The only penalty for failure to comply with Real ID is that the citizens of non-compliant states cannot use their drivers' licenses to board airplanes or enter federal facilities. If DHS were to implement Real ID, it would mean denying the 64.7 million citizens of these 15 states, more than 20% of the total U.S. population, the right to use their drivers' license when boarding an airplane.[4] Because a state driver's license is the main identification for most Americans this is functionally impossible. DHS would either have to ignore the aviation identification requirement altogether or send millions of people to secondary screening or employ other, much slower, mechanisms for verifying identity. The first alternative has already been rejected by DHS on security grounds. The other two would bring air travel to a halt and cause numerous security problems at other federal facilities.

The only viable alternative is the one DHS has chosen: to postpone implementation repeatedly. According to the original language of the Real ID Act, its provisions were to be implemented within three years, by May 2008. In January 2008, DHS postponed that deadline, creating two new compliance deadlines. States were required to be compliant with one part of the act by December 31, 2009 and be fully compliant by May 11, 2011.[5] Those deadlines again proved impossible and further extensions were granted in December 2009 and January 2011.[6] The current nominal compliance deadline has been extended to January 2013.[7]

Given such facts regarding Real ID implementation and the current impasse between the federal government and the states, any further regulatory efforts by DHS are futile. It is incumbent upon Congress and DHS to recognize that any further actions around a statute that will never be implemented is wasteful and unnecessary. DHS should halt any further Real ID rulemaking and Congress should repeal the underlying Real ID statute.

---

[4] U.S. Census Bureau. (2010, December 21) *Resident Population Data* (retrieved October 28, 2011).
[5] 73 Fed. Reg. 5272.
[6] 74 Fed. Reg. 68477.
[7] 76 Fed. Reg. 12269.

962 Wayne Avenue, Suite 701
Silver Spring, MD 20910
(301) 563.6001 Fax: (301) 563.6012

NATIONAL ASSOCIATION FOR PUBLIC HEALTH STATISTICS AND INFORMATION SYSTEMS

President
MARK FLOTOW
Illinois

President Elect
JENNIFER WOODWARD, PhD
Oregon

Treasurer
BRUCE COHEN, PhD
Massachusetts

Secretary
KELLY BAKER, MPH
Oklahoma

Member at Large
JAMES EDGAR, MPA
Montana

Member at Large
RICHARD MCCOY, MPA
Vermont

Member at Large
ELIZABETH W. SAADI, PhD
Kansas

Member at Large
LINETTE T. SCOTT, MD, MPH
California

Past President
ISABELLE HORON, DrPH
Maryland

Executive Director
GARLAND LAND, MPH
NAPHSIS

March 22, 2012

The Honorable James Sensenbrenner, Chairman
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
U.S. House of Representatives

The Honorable Bobby Scott, Ranking Member
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
U.S. House of Representatives

Dear Chairman Sensenbrenner and Ranking Member Scott:

The National Association for Public Health Statistics and Information Systems (NAPHSIS) thanks you for scheduling the subcommittee's important and timely hearing, "Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards," and we were pleased to submit a statement for the record on the role of vital records and the Electronic Verification of Vital Events (EVVE) system used to safely and securely verify the authenticity of birth certificates.

During the hearing, witnesses were unable to answer your specific questions about birth certificates—how does one obtain a birth certificate, and what do they need to present to obtain it? NAPHSIS would like to take this opportunity to respond to your questions on the record as the organization that represents the 57 vital records jurisdictions that collect, process, and issue birth and death records in the United States.

Vital records are permanent legal records of life events, including live births, deaths, fetal deaths, marriages, and divorces. Data providers—for example, hospitals for birth information and funeral homes, physicians, and coroners for death information—submit birth and death data to the vital records jurisdictions so that the vital event can be reviewed, edited, processed and officially registered. The jurisdictions are then responsible for maintaining registries of such vital events and for issuing certified copies of birth and death records.

The 57 vital records jurisdictions, not the federal government, have legal authority for the registration of these records, which are thus governed under state laws. The laws governing what information may be shared, with whom, and under what circumstances varies by jurisdiction. In most jurisdictions, access to records is restricted to family members for personal or property rights, to government agencies in pursuit of their official duties, or for research purposes. In other jurisdictions, release of vital records information may be subject to less restrictive limitations; and in a few states identifiable information from birth and death certificates is publicly available.

To obtain a copy of a birth certificate, an individual must complete an application and submit it to their state of birth by mail, or in-person at designated walk up counters. Some states now accept applications online. In most cases, an individual wishing to purchase a copy of a birth certificate must also present a driver's license with the application, or if not applying in person, a copy of it.

True identification of an individual seeking a birth certificate is difficult, and a careful vetting requires significant time and highly trained staff. At present, most vital records jurisdictions do not have the resources and the needed technological solutions to verify the identity of purchasers, track "repeat customers," and investigate suspicious activity. In the majority of states, most vital records are purchased by mail. Unlike obtaining a driver's license, where the driver is always present in the state, many people live far from the site where the records are kept and certified copies are issued, often in a different state or country. Such transactions make purchaser identification even more difficult, as copies of proxy identification documents are easy to fake, and comparisons of an individual with a picture are not possible. The true intent of the purchaser is virtually impossible to determine.

As mentioned in our written statement for the record submitted March 21, 2012 in conjunction with the hearing, the Department of Homeland Security is in the earliest stages of supporting a new project to close some of these loopholes that contribute to identity fraud. In this "reciprocal pilot," three departments of motor vehicles (DMV) will use the EVVE system to verify birth certificates, and three vital records jurisdictions will use the DMVs' driver's license verification system to verify driver's licenses that individuals present to obtain copies of birth certificates. The development of the interface should take about one year and once installed, the pilot will last 14 months. During the pilot, the DMVs and vital records jurisdictions will jointly investigate instances of "no matches," determining why a no match occurs and developing business practices to handle no matches.

NAPHSIS's *White Paper on Recommendations for Improvements in Birth Certificates* includes a comprehensive set of remedies for these and other birth certificate vulnerabilities consistent with the 2004 Intelligence Reform and Terrorism Prevention Act. These recommendations reflect our professional judgments on the amount of security and fraud risk that will be alleviated, the ease of implementation, the resources required, and the need for coordination with other entities outside the vital records community. In summary, NAPHSIS recommends that long-delayed regulations—expected September 2012 from the Department of Health and Human Services—on birth certificate issuance standards include provisions to strengthen birth certificate security, printing, use, and release requirements. More broadly, NAPHSIS recommends support for the modernization of the vital records infrastructure to produce more accurate, timely, and secure vital records. Specifically, HHS' investment in electronic birth and death registration systems will secure these records as intended by the Intelligence Reform and Terrorism Prevention Act, and will benefit HHS as it performs its key functions.

To obtain a copy of a birth certificate, an individual must complete an application and submit it to their state of birth by mail, or in-person at designated walk up counters. Some states now accept applications online. In most cases, an individual wishing to purchase a copy of a birth certificate must also present a driver's license with the application, or if not applying in person, a copy of it.

True identification of an individual seeking a birth certificate is difficult, and a careful vetting requires significant time and highly trained staff. At present, most vital records jurisdictions do not have the resources and the needed technological solutions to verify the identity of purchasers, track "repeat customers," and investigate suspicious activity. In the majority of states, most vital records are purchased by mail. Unlike obtaining a driver's license, where the driver is always present in the state, many people live far from the site where the records are kept and certified copies are issued, often in a different state or country. Such transactions make purchaser identification even more difficult, as copies of proxy identification documents are easy to fake, and comparisons of an individual with a picture are not possible. The true intent of the purchaser is virtually impossible to determine.

As mentioned in our written statement for the record submitted March 21, 2012 in conjunction with the hearing, the Department of Homeland Security is in the earliest stages of supporting a new project to close some of these loopholes that contribute to identity fraud. In this "reciprocal pilot," three departments of motor vehicles (DMV) will use the EVVE system to verify birth certificates, and three vital records jurisdictions will use the DMVs' driver's license verification system to verify driver's licenses that individuals present to obtain copies of birth certificates. The development of the interface should take about one year and once installed, the pilot will last 14 months. During the pilot, the DMVs and vital records jurisdictions will jointly investigate instances of "no matches," determining why a no match occurs and developing business practices to handle no matches.

NAPHSIS's *White Paper on Recommendations for Improvements in Birth Certificates* includes a comprehensive set of remedies for these and other birth certificate vulnerabilities consistent with the 2004 Intelligence Reform and Terrorism Prevention Act. These recommendations reflect our professional judgments on the amount of security and fraud risk that will be alleviated, the ease of implementation, the resources required, and the need for coordination with other entities outside the vital records community. In summary, NAPHSIS recommends that long-delayed regulations—expected September 2012 from the Department of Health and Human Services—on birth certificate issuance standards include provisions to strengthen birth certificate security, printing, use, and release requirements. More broadly, NAPHSIS recommends support for the modernization of the vital records infrastructure to produce more accurate, timely, and secure vital records. Specifically, HHS' investment in electronic birth and death registration systems will secure these records as intended by the Intelligence Reform and Terrorism Prevention Act, and will benefit HHS as it performs its key functions.

OFFICE OF THE GOVERNOR
STATE OF MONTANA

BRIAN SCHWEITZER
GOVERNOR

JOHN BOHLINGER
LT. GOVERNOR

March 21, 2012

The Honorable James Sensenbrenner
Chairman
Subcommittee on Crime, Terrorism, and Homeland Security
House Judiciary Committee
B-370B Rayburn House Office Building
Washington, DC 20515

The Honorable Louie Gohmert
Ranking Member
Subcommittee on Crime, Terrorism, and Homeland Security
House Judiciary Committee
B-370B Rayburn House Office Building
Washington, DC 20515

Dear Chairman Sensenbrenner and Ranking Member Gohmert,

I write in strong opposition to the REAL ID Act.

In 2005, I signed a law forbidding Montana from complying with REAL ID (MCA 61-5-128). This law stated that Montana found the REAL ID to be "*inimical to the security and well-being of the people of Montana, will cause unneeded expense and inconvenience to those people, and was adopted by the U.S. congress in violation of the principles of federalism contained in the 10th amendment to the U.S. constitution.*"

Montana objects to the implementation of REAL ID for a number of reasons, the most important of those being its threat to our privacy rights which are enshrined in our 1972 Constitution. The so-called national identity verification hub, and the arbitrary demand that Montanans show a "REAL ID compliant document" before boarding a commercial flight or entering a federal building, are direct threats to Montanans' individual rights and privacy.

Montana will not agree to share its citizens' personal and private information through a national database, nor bear the exorbitant cost building such a database. Furthermore, the Act tramples on our state's right to determine our own licensing procedures and protocols, and would interfere with our state's work to improve drivers' license security.

Montana is in no mood at all for another heavy-handed play by the federal government, such as what transpired in 2008 when the homeland security director threatened to prevent Montanans from boarding an airplane unless we complied with the REAL ID act. We refused, and will refuse again.

While folks in Washington may have believed they knew what was best for Montana when they created the REAL ID Act, in fact, Montanan's have little use for this unpopular, unfunded, and completely unfeasible mandate. The House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security should use today's hearing to begin the process of repealing the REAL ID Act.

Sincerely,

BRIAN SCHWEITZER
Governor

STATE CAPITOL • P.O. BOX 200801 • HELENA, MONTANA 59620-0801
TELEPHONE: 406-444-3111 • FAX: 406-444-5529 • WEBSITE: WWW.MT.GOV

NATIONAL
FRATERNAL ORDER OF POLICE®

328 MASSACHUSETTS AVE., N.E.
WASHINGTON, DC 20002
PHONE 202-547-8189 • FAX 202-547-8190

CHUCK CANTERBURY
NATIONAL PRESIDENT

JAMES O. PASCO, JR.
EXECUTIVE DIRECTOR

26 March 2012

The Honorable F. James Sensenbrenner, Jr.
Chairman
Subcommittee on Crime, Terrorism and
Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Robert C. Scott
Ranking Member
Subcommittee on Crime, Terrorism and
Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman and Representative Scott,

I am writing on behalf of the members of the Fraternal Order of Police to provide you with our views on the REAL ID Act, which is the subject of an oversight hearing entitled, "Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards."

The Fraternal Order of Police has supported the REAL ID Act since it was initially proposed in 2005 because, for our members, it is a critical officer safety issue. Whether it's a routine police matter or a life threatening situation like an auto collision, law enforcement officers rely on identity documents to establish the identity of the persons involved. In nine out of ten instances, that identity document is a driver's license. Driver's licenses also allow officers to access information related to a person's driving record, and more importantly, any criminal history. In states that now comply with REAL ID rules, hundreds of criminals are being uncovered as imposters by police officers working with the driver's license agencies. Some of those imposters are identity thieves, and others are wanted criminals with violent histories.

The new rules implement Federal law by setting specific requirements for States to help combat identity fraud. New licenses can only be issued after an individual's identity and proof of citizenship or legal status have been established and all new licenses must incorporate information and security features. For example, the States of Ohio, Florida, and Delaware, all of which are compliant with REAL ID, have brought charges against hundreds of imposters for fraud and identity theft. Finding these imposters also makes the road safer. Last year, fifty four percent of identity theft suspects arrested by the Ohio State Highway Patrol were also charged with having a suspended license. Fifteen percent of suspects were charged with operating a vehicle under the influence impaired.

This data demonstrates what the FOP maintained during the debate to enact this legislation--improving the security of identity documents like driver's licenses can help us get criminals off the street. In States like Maryland, where driver's license security is being raised to meet REAL ID

standards, there have been numerous arrests for identity fraud uncovered by investigators. Driver's license agencies can play a significant role in assisting law enforcement officers as they investigate identity crimes or organized criminals using falsified identity documents to fraudulently obtain other identity documents.

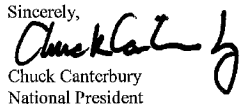
Complying with REAL ID standards also make it much more difficult fo criminals to obtain and exploit counterfeit driver's licenses. In particular, the "invisible" security features known only to law enforcement are incredibly important to combat high quality counterfeits which are finding their way into the United States in larger numbers. At the end of the day, the security of our nation's driver's licenses is only as strong as its weakest link. Organized criminals will target and exploit systems which allow them greater and easier access to fraudulent or illegally obtained documents.

Cost was one of the genuine concerns raised about the implementation of the REAL ID Act. Happily, we are given to understand that the actual cost for implementation is much lower than the estimates made by groups like the National Governors' Association, the National Council of State Legislatures, the American Association of Motor Vehicle Associations and even those of the U.S. Department of Homeland Security.

The Fraternal Order of Police strongly believes public safety on our nation's highways and neighborhoods will be better served if the Federal government continues to support implementation of the REAL ID Act and assists all States in reaching compliance.

On behalf of the 330,000 members of the Fraternal Order of Police, thank you for holding this hearing on this important issue and for considering our views. The rank-and-file law enforcement officers who put themselves in harm's way everyday must have confidence in the identity documents they receive while doing their jobs and we believe REAL ID implementation will provide that confidence. If I can be of any additional assistance, please do not hesitate to contact me or Executive Director Jim Pasco at my Washington office.

Sincerely,



Chuck Canterbury
National President

NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

Stephen Morris
Senate President
Kansas Senate
President, NCSL

Michael P. Adams
Director, Strategic Planning
Virginia Senate
Staff Chair, NCSL

William Pound
Executive Director

STATEMENT OF THE
National Conference of State Legislatures

REGARDING

The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards

TO
The Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United State House of Representatives

March 21, 2012

Denver
7700 East First Place
Denver, Colorado 80230
Phone 303.364.7700 Fax 303.364.7800

Washington
444 North Capitol Street, N.W. Suite 515
Washington, D.C. 20001
Phone 202.624.5400 Fax 202.737.1069

Website www.ncsl.org
Email info@ncsl.org

On May 11, 2005, Congress passed the REAL ID Act as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act (P.L. 109-13), creating national standards for the issuance of state driver's licenses and identification cards. While state legislators across the country share the goal of ensuring the security and integrity of state-issued driver's licenses and identification cards, the road to successful implementation of REAL ID has been impeded by a number of implementation obstacles, which remain unresolved. This includes:

- the federal government's failure to fully fund the REAL ID requirements;
- uncertainty regarding the availability of, connectivity to and governance structure for use of a number of databases that states will need to access in order to electronically verify the validity of identity documents;
- the uncertainty regarding privacy protections; and
- the Department of Homeland Security's (DHS) failure to recognize the critical role of state legislatures in implementation of the REAL ID.

Failure to Fund

Congress has provided less than $225 million to states for REAL ID implementation—a $3.9 billion mandate, according to the DHS cost estimate. States have collectively closed $480 billion in budget gaps between fiscal years 2009-2012 and also face further significant reductions in federal funds as a result of the Budget Control Act. States do not have extra funds to pay for federal mandates and to make implementation of REAL ID an allowable expense under other homeland security programs is not a solution. States must also not be required to pay to access the databases/systems necessary to verify the validity of certain identification documents. (*See Databases/Privacy Protections*.) Congress needs to fully fund the requirements or provide states relief from implementation through the use of waivers, extensions, and changes to the law or final regulations.

Databases/Privacy Protections

The REAL ID Act and its implementing regulations require states to verify the validity of identification documents presented by individuals applying for a REAL ID compliant credential with the issuer of the document. When fully implemented, this process will require states to have access to at least five national databases. While some of these databases exist, the availability and reliability of a number of these databases has yet to be tested on a national level. In addition, for several of these databases, the method by which states will connect to these systems and the governance structure for information sharing has yet to be resolved. The uncertainty regarding these systems makes it difficult for state legislators to respond to questions they receive from their constituents regarding privacy: "Who will have access to my

information?" "How will it be protected?" "Is this a national database?" These issues need to be resolved, with input from state legislators, before states are required to implement the requirements.

State Legislatures' Role

The lack of understanding by DHS, the current and previous administration, of the critical role of the state legislature in the implementation of REAL ID—appropriating funds, oversight, evaluation, information gathering activities— has been a barrier. The National Conference of State Legislatures encourages the department to engage in additional outreach to state legislatures as the full implementation deadline approaches.

NCSL Policy

In response to the implementation obstacles discussed, the following policy was adopted unanimously at NCSL's 2011 Legislative Summit.

> *NCSL urges Congress and the administration to continue to work with NCSL and its members on alternatives to the REAL ID. NCSL supports efforts to extend existing deadlines until obstacles to implementation are addressed. In addition, NCSL supports the use of waivers by the Secretary of the Department of Homeland Security, for states that have adopted other forms of compatible identification.*
>
> *NCSL urges Congress and the administration to work with NCSL and its members to adjust Title II of the REAL ID Act and develop solutions in conjunction with NCSL that recognize national security but do not impede the sovereignty of state licenses or place a federal agency or agent as a permanent and ongoing authority for determining state license uses and requirements.*

The Need for Change

NCSL supported congressional efforts in 2009 (PASS ID—*Providing for Additional Security in States' Identification Act of 2009*) to make changes to the REAL ID and would welcome legislative or regulatory efforts by the 112th Congress or the administration, respectively, to address the acts implementation obstacles. NCSL urges Congress and the department to engage state legislators in this process.

With less than 10 months until the REAL ID full compliance deadline, state legislators remain committed to working with federal policymakers on this issue. State legislators share your common goal, to ensure the safety and security of our nation.

Attachment: State Legislative Activity in Opposition to the Real ID

State Legislative Activity in Opposition to the Real ID

Statutory Opposition to Comply with the Real ID	Approved Concurrent or Joint Resolutions in Opposition to the Real ID[1]
Alaska - 2008 SB 202	Arkansas - 2007 SCR 16, SCR 22
Arizona - 2008 HB 2677; 2009 HB 2426	Colorado - 2007 HJR 1047
Georgia[2] - 2007 SB 5	Hawaii - 2007 SCR 31
Idaho - 2008 HB 606	Illinois - 2007 HJR 27
Louisiana - 2008 HB 715	Nebraska - 2007 LR 28
Maine - 2007 LD 1138	Nevada - 2007 AJR 6
Minnesota - 2009 HB 988	North Dakota - 2007 SCR 4040
Missouri[3] - 2009 HB 361	South Dakota - 2008 SCR 7
Montana - 2007 HB 287	
New Hampshire - 2007 HB 685	**Approved House or Senate Resolutions in Opposition to the REAL ID**
Oklahoma - 2007 SB 464	Michigan - 2007 HR 176
Oregon[4] 2009 SB 536	Pennsylvania - 2008 HR 767, SR 126
South Carolina - 2009 SB 449	
Utah – 2010 HB 234	
Virginia[5] - 2009 HB 1587, SB 1431	
Washington[6] - 2007 SB 5087	

[1] Does not include states that have adopted both statutes and resolutions in opposition to the Real ID. Those states are only listed as states adopting statutes in opposition to the REAL ID.

[2] Allows the Governor to delay Real ID compliance until the U.S. Department of Homeland Security guarantees that defined safeguards will protect the economic and biological privacy of the citizens of Georgia.

[3] Prohibits the Department of Revenue from amending procedures for applying for a driver's license or identification card in order to comply with the goals or standards of the federal Real ID Act of 2005, any rules or regulations promulgated under the authority granted in such act, or any requirements adopted by the American Association of Motor Vehicle Administrators for furtherance of the act. Contains other provisions regarding driver's licenses and identification cards

[4] Became law without the Governor's signature. Prohibits any state agency from expending any funds to implement the Real ID Act unless the state DOT implements sufficient measures to protect individuals privacy, and puts safeguards in place that protect against the unauthorized disclosure or use of an individual's personal identifying information. The DOT cannot participate in the Real ID Act if it: requires the department to participate in any multistate or federal shared database program unless the department is able to provide sufficient security measures to protect the privacy of individuals; charges unreasonable fees; or place unreasonable record keeping burdens on an applicant for issuance, renewal or replacement of a driver license, driver permit or identification card. Requires the state DOT to prepare a report that analyzes the cost of the Real ID Act to the state, which has to be available to the state.

[5] Prohibits implementation to comply with any provision of the Real ID Act and with any other federal law, regulation, or policy that would compromise the economic privacy, biometric data or biometric samples of any resident of the Commonwealth.

[6] Prohibits implementation unless changes are made regarding privacy and funding.

About NCSL

The National Conference of State Legislatures (NCSL) is the bipartisan organization that serves the legislators and staffs of the states, commonwealths and territories. NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues and is an effective and respected advocate for the interests of the states in the American federal system.

NCSL has three objectives:

- To ensure state legislatures a strong, cohesive voice in the federal system.
- To improve the quality and effectiveness of state legislatures.
- To promote policy innovation and communication among state legislatures.

The Conference operates from offices in Denver, Colorado, and Washington, D.C.

Contact:

Molly Ramsdell, Director, Washington Office
National Conference of State Legislatures
444 North Capitol Street, NW, Suite 515
Washington, D.C. 20001
Phone: 202-624-5400
Email: molly.ramsdell@ncsl.org

93RD DISTRICT
STATE CAPITOL
P.O. BOX 30014
LANSING, MI 48909-7514
PHONE: (517) 373-1778
FAX: (517) 373-5780
E-MAIL: paulopsommer@house.mi.gov

MICHIGAN HOUSE OF REPRESENTATIVES
PAUL E. OPSOMMER
STATE REPRESENTATIVE

Written Statement of Paul Opsommer
Chair, Michigan House Transportation Committee

to the

Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

U.S. House of Representatives

"Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards"

March 21, 2012

Chairman Sensenbrenner, Ranking Member Gohmert, distinguished members of the committee; my name is Paul Opsommer, Chair of the Michigan House Transportation Committee. During the past 5 years I have been heavily involved in REAL ID, passing state level resolutions and bills within Michigan, as well as drafting adopted related policy with the National Conference of State Legislators. I appreciate the opportunity to present to you my personal written testimony regarding state implementation of Title II of the REAL ID Act.

OVERVIEW:

Michigan is one of many states that has not passed legislation to comply with the REAL ID Act, and our laws contain statutory language that nothing in its driver's license code authorizes compliance with Title II of REAL ID. While some of the intent and requirements of Title II are well intended, it is my opinion that there are better ways to obtain the core objectives of the most basic best practices called for under the first round of final rules. Please note that while Michigan is in some cases technically compliant with some aspects of REAL ID, these have been accomplished on our own initiative, independent of REAL ID, and should not be construed as a willingness or desire to continually have our driver's license standards set by the federal government. Indeed, our experience with another DHS program, known as Enhanced Driver's Licenses (EDLs), has proven that many of the concerns about giving ongoing power to federal bureaucratic processes are not hypothetical and are indeed a real danger and concern to the states and its citizens. While I sincerely appreciate the work of the many people who, like me, seek the best public policy that balances the safety of our citizens with the tenets of freedom, federalism, and state powers, I believe that Title II of REAL ID needs to be repealed and replaced.

BACKGROUND:

As you are no doubt aware, when the REAL ID Act was passed it replaced a negotiated rulemaking process that was already taking place with the states in this area. This was controversial for several reasons, primarily because early versions of the REAL ID law would have required states to join the AAMVA compact known as the Driver's License Agreement (DLA). Such a requirement would have not only put an international 501c3 with foreign voting members in charge of driver's license provisions in regards to technology and biometrics, it would have also mandated international data sharing. While this provision is not in the current set of rules, because DHS control under REAL ID is permanent and ongoing there is little solace to the states in this area knowing the direction some would like to take future rulemaking. Likewise, although advanced biometric collection and RFID were not called for in the current rulemaking process, the current rules expressly state that DHS can change these requirements at any time and would not need to go back to Congress in order to do so.

As an example:

> **Page 86, "Moreover, in the future, DHS, in consultation with the States and DOT, may consider technology alternatives to the PDF417 2D bar code that provide greater privacy protections after providing for public comment"**

The "final rules" are therefore not really final, and it is unacceptable that such technological decisions could be made by requiring only non-binding consultation with States, especially when there is debate between the States and the federal government as to what really constitutes optimal privacy and security options for their driver's licenses.

Contrary to other reports or testimony you may receive, after talking to my colleagues both here in Michigan and across the country I strenuously assert that the states do not see tremendous value in keeping Title II of REAL ID in its current form that abrogates all state powers. Michigan, on its own accord and through its own initiatives, has denied drivers licenses to illegal immigrants. We have other strong security measures in place that we fully support and are proud of. These are state policy positions we are pursuing on our own, irrespective of REAL ID. Any reports that show states like Michigan as somehow being supportive of the REAL ID law itself because it has made similar decisions only shows the initiative the states have in this area. In fact, many of these same states ironically have laws on the books expressly prohibiting them from complying with REAL ID.

In fact, no state could currently reach all REAL ID benchmarks today even if they wanted to, because some database requirements have not been finalized. Even for those states that are currently receiving a gold star for "technical compliance", not all benchmarks are being met. In the future, DHS may very well ask them to remove the gold stars from their licenses, a bureaucratic nightmare in of itself. What will constitute earning a gold star will continue to be a moving target, and once states start to issue these there will be tremendous pressure to go along with all future requirements considering the cost to reissue new noncompliant licenses. Because this is not taking place as a finite rulemaking process with the states, I do view this as a federal takeover and as an outsourcing of a defacto national ID card onto the states. In my opinion, while each license will continue to have a unique state look and design, it will be a national ID card that would come in over 50 assorted flavors with nothing more than a prominent state designation data field. There does not need to be a federal database to have a national ID card.

As final background, I would like to share my experience of the past several years dealing with the Department of Homeland Security regarding what are known as Enhanced Driver's Licenses (EDLs). While Michigan has entered into this program, one that was initially presented to us as a non-cookiecutter partnership with the federal government, we currently have significant buyer's remorse. As an example, DHS is mandating the we issue EDLs that include unencrypted, long range (20-30 feet) RFID chips in our EDLs despite the fact they acknowledge this was not a requirement of Congress. While a debate on the ramifications of such technology and unmanned automated checkpoints is not appropriate here, it shows how quickly bureaucratic

rules, both official and unofficial, creep into seemingly innocuous programs. Michigan's Secretary of State has presented to DHS a new EDL agreement that would allow for the continuance of an EDL program in every secure manner, that verifies and denotes citizenship, but does not contain a wireless chip. This is what Congress intended. Such attempts have been repeatedly and firmly denied however, and I would advise other states not to adopt EDLs until this is resolved.

I also unfortunately believe this to be indicative of how DHS will treat the states in a similar manner under both current and future REAL ID rules and rulemaking processes. These will be decisions on collecting advanced biometrics / use of facial recognition, use of wireless technology, the sharing of data with foreign governments, and additional potential federal uses such as medical care or firearm purchases.

SOLUTIONS AND CONCLUSIONS:

Title II of the REAL ID Act as currently written is unworkable and needs to be repealed and replaced. Most states have already adopted what I consider to be the "low hanging" security standards we should implement. A negotiated and finite rulemaking process with the states would not undo any of the good work that has already been done, and would allow the states to go forward with federal partnerships knowing they are not being forced to give a virtual blank check to the federal government or its agents.

I also believe that beyond these basic minimum standards that Congress should keep state and federal documents separate. Indeed, the federal government would be well served by focusing on its own federal passport standards, some of which I believe are weaker than what they are requiring of the states. An emphasis should also be made to keep full-fledged federal passport costs down, a goal that numerous GAO reports have shown to be routinely ignored. "Passport-lite" cards are not the answer. Fully functional federal passports at under $50 should be a goal of Congress if it wishes to pursue laws such as the Western Hemisphere Travel Initiative. The use of behavioral economics to create demand for REAL ID and EDLs creates friction with the states, which should be viewed as equal sovereign partners.

Continued games of bluff and public relations campaigns between the federal government and the states over REAL ID deadlines are counterproductive and have become distractions hindering government from reaching real solutions for the people we seek to serve. While the REAL ID debate has become sometimes contentious, I again do thank all stakeholders for their hard work and dedication as we seek public policy that balances the safety of our citizens with the tenets of freedom, federalism, and state powers.

NASPO
204 E Street NE
Washington DC 20002
202-547-6340
www.giuffrida.org

F A X

To: US House of Representative Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security
Fax number: 202-225-5302

From: Marie Fournier
Fax number: 202-547-6348

Date: 3/20/2012

Regarding:
The REAL ID Act's Minimum Standards

Comments:

US House of Representative Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security
Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards

Prepared Comments of the North American Security Products Organization (NASPO),
ANSI Accredited Standards Developer
Michael O'Neil, Executive Director

Subcommittee on Crime, Terrorism, and Homeland Security
Secure Identification: The REAL ID Act's Minimum Standards for Driver's Licenses and Identification Cards
Wednesday 3/21/2012 - 10:00 a.m.
2141 Rayburn House Office Building
Washington, DC

Chairman Rep. Sensenbrenner, Vice Chairman Rep. Gohmert and Ranking Member Rep. Scott, thank you for the opportunity to submit the comments of the North American Security Products Organization (NASPO) in support of the Real ID ACT to the Subcommittee. We support the work of this Subcommittee in strengthening the security of primary identity documents and in particular state issued driver's licenses and identity cards under the Real ID Act.

We would like to share our thoughts on the use of recognized national and international standards in implementing security practices and procedures for the procurement, production and distribution of security sensitive documents and materials, including but not limited to Driver's Licenses and Identity Cards. The NASPO Security Assurance Standard supports these security practices and procedures in both procurement and issuance.

NASPO's Role in REAL ID
Quoting the REAL ID Security Plan Guidance Handbook: *"If the contractor's facility is accredited at Level II of ANSI/NASPO –SA-v3.0P-2005, DHS will deem that it provides all necessary physical security as long as that accreditation remains current. However, DHS does not require an ANSI/NASPO accreditation."*

About NASPO
The North American Security Products Organization (NASPO) is an initiative of public/private sectors and is supported intellectually and financially through the members of the North American Security Products Organization, a nonprofit 501 (c) (6) organization.[1] It is accredited as an American National Standards Institute (ANSI) Standards Developer Organization (SDO). It also develops standards at an international level through the International Standards Organization (ISO) under ISO Technical Committee 247, "Fraud, countermeasures and controls". NASPO as a representative of ANSI and the United States holds the position of Secretary to that committee.

[1] NASPO is an ANSI-accredited standards development organization based in Washington, D.C. NASPO maintains the ANSI/NASPO Security Assurance standard (ANSI/NASPO-SA-2008) and certifies organizations to one of three levels of security assurance. On behalf of ANSI, NASPO acts as secretariat of the International Organization for Standardization (ISO) Technical Committee on Fraud Countermeasures and Controls (ISO TC 247). NASPO also administers the ANSI-accredited United States Technical Advisory Group to ISO/TC 247 and ISO PC 246. NAPSO has recently launched a consensus body supporting the creation of an American National Standard (ANS) to define minimum standards for proof and verification of personal identities, NASPO Identity Verification and Proofing Standard (IDV-P). www.nasoe.info

The ANSI/NASPO Security Assurance Standard

The ANSI/NASPO Security Assurance Standard is one of the first security assurance standards to be recognized by the American National Standards Institute and represents one of the most holistic security standards developed to date. Based upon the principles of risk analysis it addresses multiple areas of risk that are present within the framework of most organizations, both private and public sector. While outlining the areas of risk that must be addressed it also provides for the flexibility of solution in mitigating those risks. In effect it allows multiple solutions so as not to create a fixed barrier that can be easily identified and subverted. The standard was also developed as a compliance standard that is supported by an audit and certification process. This has created an expanding system of certified contractors that provides a recognized structure of security compliant suppliers to support private, state and federal procurement process as well as legislative compliance. This reduces the risk that critical technologies will be compromised through the lack of sufficient security practices.

REAL ID Act

When the Intelligence Reform and REAL ID Acts were written their authors were mindful that it was necessary to address both document fraud as well as issuance fraud. The final rule of the Real ID Act specified numerous actions to be taken by DL/ID card issuing operations to ensure that vulnerabilities to insider fraud and intrusion are properly detected and controlled. Neither of these Acts, however, directly addressed security practices and procedures that are necessary to provide a REAL ID Compliant Drivers License (CDL). These critical security practices needed to be established to protect manufacturing operations, security material procurement and issuance from being compromised. The REAL ID Office through the development of the REAL ID Security Plan Guidance Handbook[2] has addressed many of these issues. The recommended use of the ANSI/NASPO Standard for the compliance of contractor's facilities has further supported the work of the REAL ID Office and aided the implementation of the Act for the State Issuing agencies.

Currently a great number of the States, including California and New York, have required certification to the ANSI/NASPO Standard to fulfill the contractor security requirements. By the use of a nationally recognized security standard with a compliance structure, the states have been able to provide expert guidance to their contractors at least cost to the States. This has aided the implementation process as well as increased significantly the security requirements for both the production and issuance of secure State issued identities. In addition, the use of this national standard provides to the federal oversight agencies the ability to uniformly assess compliance to their requirements as well as address unique security issues.

---

[2] DHS REAL ID Security Plan Guidance Handbook. "Why We Need More Secure Driver's Licenses. Raising the standards of state-issued identification is an important step toward enhancing national security. Because a driver's license serves so many purposes (access to federal buildings, nuclear power plants, boarding aircraft, etc.), criminals and terrorists actively seek fraudulent state-issued identification."

Conformity assessment and certification are an integral part of the ANSI/NASPO security assurance standard.

The ANSI/NASPO standard is viewed as a comprehensive security assurance program. This standard was designed by the standard authority with verification of compliance in mind. As a result, NASPO offers a conformity assessment service and issues Certificates of Compliance to successful candidates. To maintain their certification status, certificate holders must successfully undergo an annual re-certification audit.

Conclusion

We believe that the use of the ANSI/NASPO Security Assurance Standard has supported the implementation of the Real ID Act. Its requirements have significantly increased the operational security of production and issuance facilities as well as addressing the need for security in the procurement of sensitive materials used as security features. It has also aided the States by providing recognized security practices at a least cost of implementation to the States.

As REAL ID Compliant Drivers Licenses become more difficult to counterfeit and authenticate, the security pressures on the manufacturing operations and security technology suppliers will increase. It is therefore imperative that the use and implementation of the REAL ID Security Plan Guidance and the ANSI/NASPO Security Assurance Standard be universally applied to curtail the effects of future attacks by criminal or terrorists elements.

North American Security Products Organization
204 E Street, N.E.
Washington, DC 20002