IDENTITY AND SECURITY:

REAL ID IN THE STATES

This joint memorial is for the purpose of sending a message to Congress and to our Congressional Delegation that the people of Idaho object to the mandates of the Real ID Act of 2005 passed by Congress. The Real ID Act of 2005 is an $11 billion unfunded mandate on the states. The Real ID Act of 2005 is a backdoor attempt to institute a national ID card as more overt attempts to create a national ID card have always failed in the past.

The Real ID Act of 2005 has serious constitutional and privacy problems. By requiring all states to issue driver's licenses to this new standard, the Federal Government is attempting to force the states to become part of a national database with 50,000 access points to sensitive data on every American Citizen. The opportunities for identify theft will multiply exponentially. Rules for implementing the Real ID Act of 2005 have not yet been promulgated by the federal government and the states are unclear as to the actual expected cost of compliance.

Idaho Joint Memorial, March 12, 2007

INTRODUCTION

REAL ID is one of the only 9/11 Commission recommendations that relies heavily on the states for implementation. REAL ID might have curtailed 9/11. REAL ID can make a difference to our national security, our economic security and our public safety – but only if fully implemented and adequately funded. To make REAL ID a reality, however, requires more than either the federal government or the states can do on their own. It requires a partnership. It also requires an acknowledgement that securing our nation’s physical and economic integrity is not just a federal responsibility; it is everyone’s responsibility. It requires a further acknowledgement that the ability to verify an individual’s true identity is one of the cornerstones of national and economic security.

The REAL ID Act stipulates that in order for a driver license or state-issued ID to serve as an identity document for entering a federal facility – including boarding a plane – the document must meet, at a minimum, the security standards spelled out in the Act. Thus states are not required to issue licenses and IDs in accordance with REAL ID, but they could be subjecting their residents to considerable inconvenience if they do not. There is no intent whatsoever under REAL ID for the federal government to assume responsibility for issuing driver licenses. That process should and will remain with each state. REAL ID seeks only to ensure that every state's process for issuing driver licenses and IDs – including the documents themselves – meets specified minimum security standards. Determining precisely what REAL ID's minimum security standards will be is the purpose of the comment period now underway as part of the Notice of Proposed Rulemaking (NPRM) issued by the Department of Homeland Security (DHS) on March 1, 2007. That process concludes on May 8, 2007.

Today, 23 state legislatures have provided some forward momentum on REAL ID. Every state's Department of Motor Vehicles (DMV) is moving towards compliance with REAL ID in at least one area, and many are in multiple areas. The state of Washington has passed legislation not only to implement REAL ID but to go beyond it by instituting biometric checks on driver license applicants. Three states − Arkansas, Arizona and Colorado − have enacted or sent to their governor a request for Congress to fully fund REAL ID, although the first two express concerns about privacy. Nineteen states have pending legislation that seeks to implement REAL ID in some fashion. Oregon, for example, has five bills pending in support of REAL ID. Six states − Illinois, Maryland, Missouri, Nebraska, New Mexico and Vermont − have more than one piece of legislation pending that seeks either REAL ID implementation or repeal.

The mission of this paper is to give the 16 states like Idaho that seek the repeal or legislation akin to the repeal of REAL ID a reason to seek out federal partnership instead. It is essential that they do so; it takes all of us − the federal government, the states and individual Americans − to make this country the stronger, better America the 9/11 Commission envisioned when it issued its final report and recommendations and staff report *9/11 and Terrorist Travel*.

WHY AMERICA NEEDS SECURE DRIVER LICENSES

At the foundation of the 9/11 Commission 'terrorist travel' recommendations on secure IDs was the basic understanding that terrorists will continue to easily assimilate within the United States as long as identity and identity document issuance processes are easily manipulated. The Commission stated:

> All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications would have assisted them in boarding commercial flights, renting cars, and other necessary activities.
> **Recommendation:** Secure identification should begin in the United States. The federal government should set standards for … sources of identifications, such as driver licenses.
> **Recommendation:** The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system wide goals in mind. (p. 390, 387)

As the 9/11 Commission noted, there was only one 9/11 hijacker who did not obtain some form of U.S. identification, whether a state-issued driver license, personal ID or both. Three of the five hijackers who crashed a plane into the Pentagon used fraudulently obtained licenses to board. The pilot of that plane had four IDs, all from different states, with at least one obtained by fraud. And if REAL ID had been in effect in 2001, the 9/11 operational ringleader and pilot that conducted the first World Trade Center suicide, Mohamed Atta, would only have been four days from having had an expired license when he was pulled over for speeding violation on July 5, 2001.

THE CASE OF UNITED 93 PILOT ZIAD JARRAH

On September 9, 2001, two days before 9/11 pilot Ziad Jarrah crashed a plane nose-first into a field in Pennsylvania, Jarrah was stopped for speeding. This could have led to trouble for him, and trouble for the entire 9/11 operation, but it did not. Instead, Jarrah simply drove away with a $270 speeding ticket. This would likely be the case today as well.

Why? Jarrah had obtained two driver licenses from the state of Florida – one on May 2 and the other on May 24, 2001. In addition, he fraudulently obtained a state-issued ID from Virginia on August 29. When he was stopped for speeding, we don't know which Florida license he presented to the officer.

Had REAL ID been in effect, Jarrah would have been limited to one active license and the officer could have checked for other violations. The officer could have checked an immigration database, which could have shown he had entered the U.S. illegally at least five times. Instead, the officer had none of this information. Jarrah got away with a ticket and he still had in his pocket the Virginia ID that he might need for the 9/11 operation. The operation remained unscathed.

The 9/11 hijackers could have done the same today. It is still possible to obtain multiple licenses and IDs because identities are not verified. It's not only possible to game the system; it's likely, because states still don't exchange information with each other regarding those holding legitimate IDs. Police officers' hands are tied when they can't cross check the ID they've been handed against any other information.

The 9/11 hijackers are not the only terrorists we know of who have taken advantage of blind spots and weaknesses in ID issuance standards. One terrorist caught in 2001 on the northern border, Nabil al Marabh, had five driver licenses and a hazardous materials permit. Mir Aimal Kansi, who killed two people outside CIA headquarters in 1993, got a Virginia driver license despite being in the U.S. illegally. These same problems exist in many states today. As long as they do, terrorists will continue to take advantage of them.

In addition to terrorists, criminals of all ilks – identity thieves, counterfeiters, deadbeat dads and underage teens seeking IDs to drive and drive – also use multiple IDs to hide their true identity from the law. In 2005 identity theft costs were at a staggering $64 billion, with $18.1 billion of that cost involving theft of a Driver License (DL) or ID. Individual consumers spend an average of 330 hours trying to undo identity theft and suffer $15,000 on average in losses. With REAL ID, identity theft will be much more difficult because of more secure IDs that will verify ID information before a DL/ID is issued and because the cards themselves will become more tamper-resistant and easier for law enforcement to determine fakes.

REAL ID ACT BASED ON AAMVA'S SECURITY DOCUMENT FRAMEWORK

On October 24, 2001 the American Association of Motor Vehicles Administrators (AAMVA) – an organization promoting information exchange, uniform practices and reciprocity, with representatives from every US and Canadian jurisdiction – passed a resolution to form a special task force to enhance the security and integrity of the driver license and ID issuance processes.

Prior to 9/11, AAMVA had a significant leadership role that included petitioning Congress in 1996 to mandate minimum standards for driver licenses. From 1999 to 2001, AAMVA worked with the National Highway Transportation Administration (NHTSA) and Congress towards creation of the Driver Record Information Verification System (DRIVerS). So when AAMVA went to work on creating a special task force to deal with the panoply of issues involved in creating a more secure ID issuance framework, the organization had the ability and credibility to make a difference. And they did. Their work became the foundation for the technical requirements of the REAL ID Act.

The Driver License/ID Security Framework that emerged from the AAMVA Special Task Force was detailed and comprehensive; that Framework became the backbone for REAL ID. The outline of the task force responsibilities is worth repeating as it shows how AAMVA – and thus the state DMVs – were well aware and desirous of fixing the multiple vulnerabilities in state ID issuances systems. In some ways, then, REAL ID was simply a federal bow to the states' own work in this area. AAMVA's 'Uniform Identification Subcommittee' divided the issues into sub-categories. What is interesting is that despite the permutation of the mission statements from these subcommittees to the AAMVA Security Document Framework, to REAL ID, to the proposed rules, much of the language and policy statements have remained relatively unchanged.

Another interesting aspect of AAMVA's tasking was a group established just to deal with enforcement issues, including those treating/ID fraud, and determine increased penalties for dealing with such fraud. A significant justification for REAL ID is that by setting minimum standards as a foundation in both the verification of identity and card production processes, security is built into all state systems. This will make law enforcement activity more effective while at the same time discouraging fraud. As Chuck Canterbury, National President of the Fraternal Order of Police stated in a Feb. 21, 2007 letter to Senate Majority Leader Harry Reid:

> [REAL ID] is very much of an officer safety issue. Law enforcement officers need to have confidence that the documents presented to them to establish the identity of a given individual are accurate. Officers rely on these documents during traffic stops and other law enforcement actions to access information related to that individual's criminal history. No police officer wants to be in the dark about the fact that he may have detained a wanted or violent criminal who has simply obtained false identification. This places both the officer and the public he is sworn to protect in greater danger. For this reason, the FOP will strongly oppose any bill or amendment that would repeal the REAL ID Act.

Below is a chart that shows that the policies advocated by the states via AAMVA's 2001 working groups remains a strong influence on REAL ID policies advocated today by DHS and also influenced by the National Governors' Association and National Conference of State Legislators. This chart reflects where AAMVA started in 2001 as closely tied to March 26, 2007 testimony by DHS Assistant Secretary for Policy Development Richard Barth before the Senate Homeland Security and Governmental Affairs Committee.

Secure ID feature tasked by AAMVA	2001 AAMVA Secure ID Issuance Task Force assignments	2007 DHS REAL ID Proposed Rules for Secure ID Issuance
Model Legislation *Process and Procedures* *Driver License Agreement* *DRIVerS Infrastructure*	'develop model legislation to assist states in implementing the overall package of Uniform Identification Standards' 'gather and incorporate all deliverables of the Uniform ID Subcommittee (Task Groups) into one Model Program. This model program will include minimum requirements, best practices and model legislation to support a uniform and secure driver license and identification card system for motor vehicle agencies in the U.S. and Canada.' 'The DLC/NRVC (Driver License Compact/Non-Resident Violator Compact) Joint Compact Executive Board has been asked to explore enhancing the newly created Driver License Agreement (DLA), a voluntary driver license compact between States, to include requirements established for a more secure DL/ID issuance system. ' 'The Driver Record Information Verification System (DRIVerS) task group will be charged with creating an all driver pointer system, to keep bad drivers off the road. Simply put, DRIVerS will direct a state where to find and accurately verify someone's driving history in another state.	REAL ID is that legislation 'At the end of the day, what does all this look like? While the rule is still pending, there is no definitive answer yet. However, the final answer is that the REAL ID standards will likely draw from all the best and most secure State practices already in place.' Richard Barth, testimony before the Senate HSGA, March 26, 2007.
Acceptable Documents *Residency*	'validate and update the existing acceptable ID document list for the proof/authentication of specific personal information, such as, name, date of birth (DOB), legal presence, etc. and evaluate the utilization of foreign documents for the same purpose. Phase two will result in a recommendation for document (DL/ID) validity periods in relation to legal status/validity' 'to develop a definition of residency/domicile	'states would require individuals obtaining driver's licenses or personal ID cards to present documentation to establish identity—U.S. nationality or lawful immigration status as defined by the Act, date of birth, SSN or ineligibility for SSN, and principal residence'

	with and without a legal presence requirement for the purpose of driver licensing (establishment of the driver control record) and identification. ‘	
Verification *Fraudulent Document Recognition*	‘identify and establish methods for verifying documents used to establish identity of an individual applying for a driver license or identification card. Verification of identity may include, but is not limited to, full legal name, date of birth, Social Security Number (when applicable), and residency and/or legal presence’ ‘to assist jurisdictions with the formal training of motor vehicle employees and law enforcement in the recognition/detection of fraudulent identification documents.’	‘states would verify the issuance, validity, and completeness of a document presented. Electronic verification proposed depending on the category of documents’ and include those to verify DOB, SSN, passport issuance and legal presence
Card Design Specifications	‘deals with physical and encoded features of the driver license / ID document. Features include security elements, card layout, printed and encoded data, and machine-readable technologies. It is our hope that this effort produces a standard for the driver license document that specifies minimum data and minimum technologies to be used on the driver license / ID document‘	‘proposal contains standards for physical security features on the card designed to prevent tampering, counterfeiting or duplication for a fraudulent purpose, and a common MRT with defined data elements’
Internal Controls	‘to identify best practices for internal fraud control and prevention measures’	*Physical Security/Security Plans*: ‘each state must prepare a comprehensive security plan for all state DMV offices and DL/ID card storage and production facilities, databases and systems and submit these plans to DHS as part of its certification package *Employee Background Checks*: for those dealing with applicant information or card production including FBI fingerprint and criminal data checks
Oversight Compliance System	‘to review current procedures for the oversight and compliance of Federal and State programs and to develop a process for compliance to AAMVA standards regarding DL/ID Processes/Procedures’	‘similar to Dept Transportation regulations governing state administration of commercial driver licenses, states must submit a certification… to demonstrate compliance with.. [REAL ID] regulation’

Unique Identifier	' developing a way to uniquely identify an individual such that: • A holder will have no more than one (1) DL/ID card and record • authorized users can verify that the holder of a DL/ID card is the individual to whom the card was issued; and • an individual's driver record contains only information that pertains to that individual.	'state-to-state data exchange for those who possess REAL ID license, extending out the CDLIS data exchange that has taken place successfully since 1992, a program that eliminated multiple licenses in multiple states by 871,000 from 1992-1996'

DEBUNKING MYTHS

Idaho's joint memorial raises issues that are being replicated in jurisdictions across the nation. They deserve answers. This section attempts to do so with the caveat that the political, technological and security frameworks which exist today continue to mature as this paper is published.

THE REAL ID ACT OF 2005 IS A BACKDOOR ATTEMPT TO INSTITUTE A NATIONAL ID CARD.

REAL ID was passed in part to do away with any notion of a National ID card. By seeking to set out minimum standards for the ID card already the ID of choice by financial, airline, entertainment and other sectors – the state-issued driver license or personal ID card – Congress made clear their intent to refrain from creating a national ID card. The only aspect of REAL ID that is national is the national interest that all states be set on a foundation of minimum standards; states can choose to meet none of them and not comply or they can choose to exceed those standards. Examples already exist on both sides of compliance, with states like Maine and Idaho currently opting out, and states like Washington already passing laws to exceed REAL ID minimum standards.

Far from calling for a national ID, fully implementing REAL ID is the best chance we have as a nation to prevent future calls for a national ID. However, implementing a national ID could become the default policy if REAL ID compliance does not occur in a comprehensive way. That makes the stakes a lot higher for all of us if states who say they will opt out actually do opt out.

THE REAL ID ACT OF 2005 HAS SERIOUS CONSTITUTIONAL AND PRIVACY PROBLEMS.

Constitutional issues

REAL ID does not usurp state power and does not violate the constitution. No state or other special interest has tried to file suit based on unconstitutionality because REAL ID requires nothing of the states. REAL ID instead imposes requirements on the federal government, requiring that only REAL ID compliant IDs be acceptable for official purposes. The NPRM limits the scope of "official purposes" of the credential to the uses specified in the REAL ID Act: (1) accessing federal facilities; (2) boarding federally-regulated aircraft; and (3) entering nuclear power plants. If states choose not to comply, DHS currently contemplates simply requiring that noncompliant state's residents carry other forms of identification for 'official purposes,' such as passports in combination with other documents.

In addition, the federal government will not issue the licenses or control the data provided by the applicants. The governance of state-to-state information exchange is completely up to the states, as well as how they decide to query any federal or private reference databases. States are already sharing best practices and moving toward standardization to enhance the security and efficiency of their processes as well as the security and quality of state-issued credentials.

DOCUMENT VERIFICATION is required under Section 202(c)(3)(A) of the REAL ID Act. All provide real time performance.

SSNs checked through SSOLV.

- Online since 1996
- Verifies name/DOB/SSN with the SSA
- Only provides match/no match information to requestor
- Averages 60,000 queries per day
- 47 jurisdictions participate
- 45 % queries processed in 1 second and 99.5% within 3 seconds
- While 87% match, the remainder do not, with 1.88% being clear fraud, or 1,128 per day on average

Vital events records checked through EVVER

- Pilot active since August 2004
- Verifies name/DOB/State of birth/record date with state Vital Records agencies via AAMVA net and EVVER network
- Over 76,000 records verified to date
- 3 states in pilot, 2 more to join in 2007, 2 others are digitized
- Match rate varies depending on state records, from 77% to 94%

Driver License/ID Card Document Verification System:

- Verifies name/DOB/DLN#/image request
- 8 states can conduct full verification, including images, and 41 others have begun the implementation process
- Relies on AAMVAnet

Immigration records checked through SAVE.

- Alien registration numbers or I-94 arrival/departure records used by states to query DHS
- States then rectify data provided by DHS with applicant records and make determination
- Currently a working group at AAMVA seeking to integrate SAVE into AAMVAnet
- Wisconsin added in April 1, 2007

Privacy issues

REAL ID will not facilitate the collection or release of personal information to or by the DMV, the federal government, nor unauthorized persons within each state. Each state must submit a privacy policy to DHS as part of their Comprehensive Security Plan, including how data will be secured against unauthorized access and procedures for its maintenance.

There are legitimate concerns that states employ best practices to protect personal data on applications, but DMVs have been dealing with that for years. In fact, under the 1994 Driver's Privacy Protection Act, states and their employees are barred from selling or releasing personal information such as Social Security numbers, photographs, addresses, telephone numbers and birthdays of applicants. The law was passed after a stalker murdered Rebecca Schaeffer, whose residential information was found through the California DMV. The statute was challenged by states who argued that Congress had overstepped its grounds by insisting upon privacy in public records and that the issue was within the states' purview. On appeal to the Supreme Court, the law was upheld under the commerce clause and the right of the federal government to regulate disclosures pertaining to privacy. This law still stands and must be incorporated into REAL ID implementation.

The dynamic for best practices of course changes and has new challenges when records go from paper to electronic. However, that is a challenge that continues to be faced – and continues to be aggressively addressed – in all electronic transactions.

On the federal level, these challenges are already being managed. When states today query both federal and private databases, authorized personnel receive responses only in defined fields of data absolutely necessary to verify essential information in regard to that particular query, whether the information sought is a SSN, a birth record, immigration or driving record. There have been no complaints that these queries and crosschecks have in any way compromised personal privacy. In fact, the checking of SSNs alone protects the privacy of legitimate applicants every day while bringing potentially illegitimate applications to attention.

The data called for on a REAL ID license is really no more than the best practices of most states. REAL ID requires that the DL or ID show the following information: full legal name, address of principal residence, digital photo, gender, date of birth; signature; issuance date; expiration date; unique document number (other than SSN); and machine-readable technology. Such information is essential for verifying identity when an ID card is presented.

VERIFYING IDENTITY AND ADDRESSING FRAUD

In 2003, the New York DMV did a cross-check of SSNs provided by DL/ID applicants against the SSA database. At least 600,000 license or ID card–holders did not jive with the SSA's database.

A recent NC internal audit showed 27,000 DL/ID applicants used false SSNs, about half 'deceased' in SSA records.

Almost every state already requires this information, or nearly all of it, and US residents are accustomed to giving and holding such data on DL/ID cards. Individual state DMVs will continue to store driver license data, as will the cards, and the federal government will have no greater access to the information than it does currently.

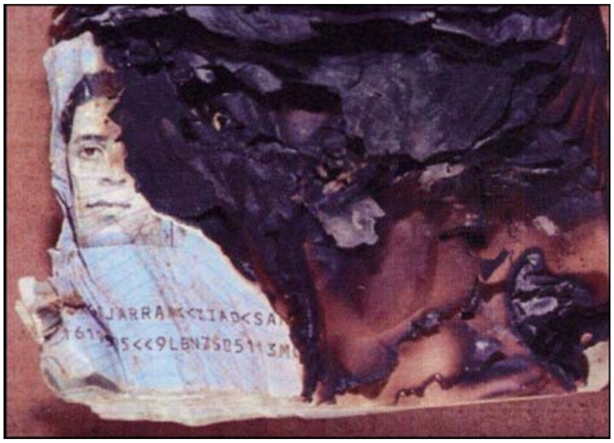
It should also be noted that the common machine-readable technology required by the Act will not convert licenses into tracking devices. There is no requirement for a radio frequency (RF)ID chip or other such device that can scan data from a distance is contemplated in REAL ID. Instead, the NPRM proposes the use of 2-dimensional (2D) bar code technology already in use today by more than 40

DMVs. The information on this bar code is typically no different from what is readable manually on the face of the card.

THE FEDERAL GOVERNMENT IS ATTEMPTING TO FORCE THE STATES TO BECOME PART OF A NATIONAL DATABASE.

REAL ID does not propose a federal database holding masses of private data. The states will continue to hold their own data. What REAL ID does require is that a state verifies with the issuing agency that each document provided to prove identity is a valid document. Birth certificates, foreign passports and immigration documents are often difficult to authenticate. The REAL ID proposed rules contemplate fast, efficient and effective means to verify such data, mainly through electronic reference libraries. Four of these libraries already exist. One is in pilot. Another has yet to be developed. What is important to note is that none of these databases hold applicant data, and only one currently uses a government network to exchange information.

The network used today and considered for expansion is the privately owned and operated AAMVAnet, which will continue to be the network conduit for information flow between most federal government databases used to verify identity and determine eligibility for REAL ID applicants. AAMVAnet already acts as the network transferring data between federal and state authorities for commercial driver license and problem driver data (CDLIS and NDR); Social Security data (Social Security OnLine Verification (SSOLV)); vital events data pilot (Electronic Verification of Vital Event Records (EVVER)); and the Driver License/ID Card Document Verification System.



A partly-burned copy of Ziad Jarrah's U.S. visa recovered from the Flight 93 crash site in Somerset County, Pennsylvania. Jarrah would have used this passport to obtain his two Florida DLs and his Virginia ID.

The only data exchanged directly between the federal government and the states right now are foreign resident legal presence checks under the US Citizenship and Immigration Service's data (SAVE), although an AAMVAnet solution is to be developed. There is current discussion that AAMVAnet would also be used for passport verification provided by the Department of State when that system is developed.

Importantly, states are already in significant compliance with many aspects of REAL ID's identity and eligibility verification requirements under REAL ID. All states are checking commercial driver and problem driver databases as required under prior federal law. All but two states are checking SSNs. Twenty states are checking for lawful presence. Vital effects (birth and death) records are in pilot within and between North Dakota, South Dakota and Iowa and five additional states have completed digitization of their vital effect records, including Hawaii, Iowa, Minnesota, Missouri and Montana. Colorado and Minnesota are scheduled to join the pilot in 2007.

What still needs to be developed are rules for data exchange between the federal and state entities, and state-to-state queries. Once again, however, this is doable, as such rules already exist for current data exchanges on driver applicants between federal and state partners. These rules can serve as the foundation for changes required under REAL ID as well, particularly those involving state-to-state exchanges. As long as the states implement this portion of the REAL ID Act, they – and not the federal government – will remain in control of the business processes. This is contemplated by DHS in their Privacy Impact Assessment that was conducted pursuant to Congressional intent and published alongside the proposed rules for REAL ID.

> The key will be to ensure that the states administer and manage the systems built to implement the Act. In addition, with appropriate and necessary participation from the affected federal agencies, including DHS, the Department of Transportation, and the Social Security Administration, the states must be empowered to develop the business rules surrounding the check of federal reference databases and the state-to-state data exchange processes. State, rather than federal, operation and control of the systems not only minimizes the appearance of a national database, but also fosters the system of federalism upon which our country is based. The language in the Preamble of the NPRM supports the important role of the states. (P.7-8)

Jurisdiction	CDLIS & NDR license checks	SSOLV (SSN)	SAVE (lawful presence)	EVVER (vital events)	Digital Image Access & Exchange
Alabama	✓	✓	✓		✓
Alaska	✓	✓			
Arizona	✓	✓			✓
Arkansas	✓	✓	✓		
California	✓	✓	✓		
Colorado	✓	✓	✓		✓
Connecticut	✓	✓			
Delaware	✓	✓			
District of Columbia	✓	✓			✓
Florida	✓	✓	✓		
Georgia	✓	✓	✓		
Hawaii	✓	✓		✓	
Idaho	✓	✓	✓		✓
Illinois	✓	✓	✓		✓
Indiana	✓	✓	✓		
Iowa	✓	✓		✓	
Kansas	✓	✓			✓

Jurisdiction	CDLIS & NDR license checks	SSOLV (SSN)	SAVE (lawful presence)	EVVER (vital events)	Digital Image Access & Exchange
Kentucky	✓	✓			✓
Louisiana	✓	✓			
Maine	✓	✓			
Maryland	✓	✓	✓		
Massachusetts	✓	✓			
Michigan	✓	✓			
Minnesota	✓			✓	
Mississippi	✓	✓			✓
Missouri	✓	✓	✓	✓	
Nebraska	✓	✓			✓
Nevada	✓	✓	✓		✓
New Hampshire	✓	✓			
New Jersey	✓	✓	✓		
New Mexico	✓	✓			
New York	✓	✓	✓		
North Carolina	✓	✓			✓
North Dakota	✓	✓	✓	✓	✓
Ohio	✓	✓			
Oklahoma	✓				✓
Oregon	✓	✓			
Pennsylvania	✓	✓	✓		✓
Rhode Island	✓	✓			✓
South Carolina	✓	✓			
South Dakota	✓	✓	✓	✓	
Tennessee	✓	✓			
Texas	✓	✓			
Utah	✓	✓			
Vermont	✓	✓	✓		
Virginia	✓	✓	✓		
West Virginia	✓	✓			✓
Wisconsin	✓	✓	✓		✓
Wyoming	✓	✓	✓		✓

But for the last column, the chart above was part of March 26, 2007 DHS testimony before the Senate Homeland Security Committee detailing identity and document verification databases currently in use or implemented in states. The 'Digital Image Access' information was provided by AAMVA in a power point presentation during a Feb. 26-27, 2007 *Paving the Way for REAL ID* conference. Note that implementation for Digital Image Access is complete in 19 states, underway in seven states and feasibility start dates are under consideration in 16 states. Only eight states have no current activity in the area of digital image access verification.

While rules for data exchange need to be developed, what is clear is that many states are well on their way towards compliance with the identity verification portion of REAL ID in a manner that does not and will not create a national database.

THE OPPORTUNITIES FOR IDENTIFY THEFT WILL MULTIPLY EXPONENTIALLY.

A collateral positive side effect of REAL ID is that it will help curtail identity theft, not enable it. For legal residents, REAL ID requires stronger security features – the details of which are available for comment in the NPRM – with the intention of driving up the cost of creating counterfeit ID documents and enabling law enforcement both working with DMVs and in the field to make a quicker, more reliable determination of whether an ID is legitimate or not.

For criminals, terrorists and others who want to live in the U.S. for nefarious purposes or under false guise, obtaining a license or ID has been their ticket to acquiring legitimate cover for their illegitimate activities. Once our identity issuance systems and the IDs themselves are tightly secured, it will be much more difficult to obtain these "tickets" fraudulently.

LAW ENFORCEMENT ACCESS TO DRIVER INFORMATION

US Law Enforcement today uses *Nlets* (International Justice & Public Safety Information Sharing Network) to exchange information regarding driver history and status for commercial and problem drivers. *Nlets* serves the law enforcement community with messaging within and between states using the Arizona Department of Public Safety facility in Phoenix. From there, all Nlets traffic is routed to federal, state and local law enforcement and state motor vehicle offices.

AAMVA has significantly upgraded the messaging on driver history and status by standardizing its definitions, content and format so that law enforcement personnel in any state can easily and quickly understand the data retrieved through *Nlets* as opposed to 51 varieties of data.

AAMVA based its recommendations on its CDLIS and PDPS systems, as commercial driver and problem drivers are already required to be reported between states by federal law.

The upgraded messaging system is in the process of being implemented, with a few states who have upgraded their systems – like New York, Maine and Wisconsin- already taking advantage of the uniform information now available via the AAMVA network on Nlets.

Adding in to *Nlets* all other driver information using proven and effective standards promulgated by AAMVA might prove helpful to REAL ID implementation and help assuage privacy concerns as well.

THE REAL ID ACT OF 2005 IS AN $11 BILLION UNFUNDED MANDATE ON THE STATES.

REAL ID does need an infusion of funds, but as stated above, it is not a mandate on states. Rather, it is a long term program that requires a long term financial support plan. For now, DHS is enabling states to use up to 20% of the state's Homeland Security Grant Program funds for REAL ID. In the last grant round, roughly $250 million was provided to states, meaning that approximately $50 million is available for REAL ID compliance.

DHS has another $34 million in another grant program expressly created for this purpose. However, that money will not be released until DHS submits its REAL ID implementation plan to Congress. That needs to be done promptly so seed money can be appropriately allocated for REAL ID implementation, and programs such as EVVER continue to expand. States already spending money on REAL ID implementation should be incentivized by a plan that rewards states with recovery cost money upon reaching goals set out for implementation.

States have estimated they need an initial $1 billion in start-up costs for REAL ID, and the total costs have been estimated at around $11 billion, although those living with the numbers think that such figures may be over-stated. More funding is absolutely required. The $300 million recently authorized by the House Homeland Security Committee is a good start, and momentum for funding should be encouraged.

RULES FOR IMPLEMENTING THE REAL ID ACT OF 2005 HAVE NOT YET BEEN PROMULGATED BY THE FEDERAL GOVERNMENT.

The NPRM is out and comments are being solicited by DHS. States and other interests with concerns need to be responsive in a timely manner so that DHS be able to issue the final rules by the end of summer 2007. Every state has been proactive in securing their DL/ID issuance processes, and each step they take brings them closer to complying with the letter and spirit of REAL ID. States and jurisdictions with strong commitment include – but certainly are not limited to – Alabama, California, Colorado, Massachusetts, Michigan, New York, Washington and Washington D.C. Many other states are planning system enhancements that will be rolled out in the next year. And for states that are further behind, the draft rules allow states to obtain extensions for compliance until December 31, 2009. However, all licenses and IDs held by individuals must be converted to REAL IDs by May 10, 2013 if a state intends to comply with REAL ID.

PUBLIC SAFETY VALUE—BEYOND REAL ID COMPLIANCE

Alabama makes about 5,000 arrests per year amongst DMV applicants. DL inspectors are trained in fraud and conduct background and security checks for applicants.

Reasons include outstanding warrants, criminal charges such as murder or escape, and expired green cards.

Texas and Connecticut also do such checks.

STATES ARE UNCLEAR AS TO THE ACTUAL EXPECTED COST OF COMPLIANCE.

The NRPM comments and the final rules DHS decides to promulgate will further refine state costs for compliance. However, the expected cost of compliance was already calculated by an AAMVA survey that became the NGA/NCSL September 2006 REAL ID Impact Study. At that time, each state was asked their current level of compliance and cost figures were drawn up as a result of those answers. States are now in a much better position to do cost estimates with the release of the NPRM on March 1, 2007.

Since the NPRM release, DHS has also released its estimates for REAL LID implementation at about $23 billion. These costs are considered high by DHS, and are expected to be lower once the final rules are released. DHS estimates also contain large soft costs, such as wait times in DMV lines for REAL ID applicants, at $7.9 billion. Although renewal times are staggered for state-issued IDs, the cost estimates to date condense this ‘wait time’ cost, thus also unfortunately exaggerating overall costs.

There are other costs included as well, including increased work load to process a REAL ID at another $6.9 billion. While work load does vary by state, the NPRM still only requires one identity document be presented from a list of nine documents proposed by DHS. What may take more time until processes are streamlined as envisioned under REAL ID, are the enhanced security processes such as authenticating documents and validating applicant information. However, REAL ID implementation is headed towards automatic, real time queries which will be fast and effective. States like Kansas, for example, have moved from an over-the-counter system to a central issuance system and have reported a decrease in applicant processing time from 14 minutes per person to seven minutes per person.

CONCLUSION

Since 9/11, every state has sought to improve its DL/ID issuance processes. Many states are quietly working towards compliance, but all have reason to comply as REAL ID is built on the familiar turf of AAMVA's long and credible history in best practices; interoperability and exchange of information between and within states using AAMVAnet; and its long relationship with the federal government in shaping legislation such as became REAL ID. While concerns over privacy and constitutional issues have emerged and will continue to be taken into consideration, these concerns that have not been borne out by the reality of the actual implementation taking place to date.

Perhaps the only real concern that is unanswerable at this time is cost. However, the $300 million authorized recently in the House is a good start, and one that needs to be replicated elsewhere in Congress. We are already far out from 9/11 without a secure DL/ID issuance system in place. The longer Congress delays funding, the more difficult it will be for states to comply in a timely manner. The one billion dollars the states requested prior to the NRPM is a good place to start – with DHS estimated costs similar – in thinking about what it will take to apportion cost fairly amongst states, taking into consideration and not penalizing those states already spending their own monies for compliance.

Yet one thing is clear: we cannot afford to undo 9/11 Commission recommendations nor the good work the states have done to date to upgrade their systems. REAL ID puts the foundation in place to grow this good work by putting in place common sense standards and best practices in a reasonable, fair way that respects both the needs and limitations of both the federal and state governments.