



## American Association of Motor Vehicle Administrators

---

Mike Calvin  
Interim President and CEO

Debra Hillmer, Chair of the Board  
Director, South Dakota Division of Motor Vehicles

May 1, 2007

The Honorable Michael Chertoff  
Office of the Secretary  
Department of Homeland Security  
Attn: NAC 1-2037  
Washington, DC 20528

**Re: Docket # DHS-2006-0030 Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Federal Purposes**

Dear Secretary Chertoff:

The American Association of Motor Vehicle Administrators (AAMVA) is filing these formal comments to Docket #DHS-2006-0030 in response to the Notice of Proposed Rule Making on Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Federal Purposes. AAMVA is filing these comments in support of and on behalf of its members who are responsible for driver's licensing and identification card issuance and who will be faced with the significant challenges of any implementation of the statute. AAMVA is very interested in ensuring that this response is considered prior to the final rule as the proposed regulations have significant cost and operational impacts to our members and the customers they serve in every motor vehicle department across the US.

Structurally, AAMVA is a professional and educational organization. Founded in 1933, the association is a member-driven organization and its voting members are state and provincial officials in the US and Canada who administer and enforce motor vehicle laws. AAMVA's non-voting membership includes associations, organizations and businesses that share an interest in advancing the organization's goals. AAMVA's mission is to represent its US and Canadian membership by working collaboratively to support and improve motor vehicle administration, safety, identification security and law enforcement in North America. While AAMVA is managed daily by a staff, it is a membership-focused organization and its actions are governed by a Board of Directors. The Board of Directors is comprised of vehicle registration & titling, driver licensing and law enforcement administrators who are experts in the business. Administration of policy, program direction and strategy are overseen by the Board of Directors. The Board of Directors is responsible for carrying out the direction of the member jurisdictions. AAMVA is drivers licensing, vehicle registration & titling and law enforcement officials who daily are responsible for safety, service and security in these areas in the US and Canada. The importance of AAMVA's membership focus is why this

**An International Safety Association of Motor Vehicle and Law Enforcement Administrators**

response to the NPRM is being signed by three signatories, the Chair of the Board for AAMVA, the Chair of the REAL ID Steering Committee and the Interim President and CEO. This response is submitted under these signatures on behalf of AAMVA's Board of Directors and its members.

AAMVA members fully recognize the importance of identification security and the need to operate a secure driver's license and identification card issuance process. AAMVA members have been engaged in this journey long before REAL ID. Work in the area of customer identification dates back to the 1980's. AAMVA members also have continued to focus on improving the security of driver license and ID cards. Directly after the 9/11 attacks, AAMVA formed a Task Force on Identification Security comprised of member jurisdictional representatives. That task force, and subsequent collaborative efforts with our federal partners, industry and organizations representing card users, resulted in the completion of a *Driver's License/Identification Card Security Framework* for all jurisdictions to use as a model to continue to improve the identification and issuance process. Many jurisdictions used this AAMVA guidance to continue to improve their licensing programs, processes and procedures in a deliberate and thoughtful manner. AAMVA members also have been actively engaged in advancing continued improvements to the licensing process and its nexus to homeland security.

In addition to driving improvements to the driver's licensing and identification card issuance process after the 9/11 attacks, AAMVA members spent countless hours analyzing and recommending improvements to the Intelligence Reform and Terrorism Prevention Act and the REAL ID Act. Some of these are reflected in the NPRM; others unfortunately are not. The knowledge and credentials of our members are well established, as they are on the front line every day.

Most recently, in September 2006, AAMVA, the National Conference of State Legislatures (NCSL) and the National Governors Association (NGA) completed a comprehensive analysis of the REAL ID Act based on the pre-regulation assumptions that existed at the time. The Report, The REAL ID Act National Impact Analysis, provided DHS with attractive solutions that would allow the Act to be implemented in a practical, economical and efficient manner. The analysis set forth the consequences and costs of implementing the Act and made recommendations to facilitate a more realistic approach. The key recommendations of the Report were:

- extend the compliance deadline since it would be impossible for states to comply with REAL ID by the May 2008 deadline
- provide funds necessary for states to comply with REAL ID since the projected cost of complying with the Act far exceeds the original Congressional Budget Office estimate and will require a more significant investment by Congress
- grant the Secretary of Homeland Security the flexibility to recognize innovation at the state level as several states have updated their systems to meet similar objectives to REAL ID. The Secretary of Homeland Security should have the discretion to recognize state practices and innovations that accomplish the goals of the Act

- implement a 10-year progressive re-enrollment schedule as it is impractical for states to renew all 245 million driver's licenses and identification cards in five years. States should be given the flexibility to delay re-verifying certain populations in order to maximize resources and avoid severe disruptions to customer service
- allow reciprocity for persons already vetted by the federal government, as states could realize significant savings and reduced transaction time if individuals whose identities have already been verified for certain federal identification cards are considered pre-qualified for REAL ID compliant driver's licenses and identification cards
- provide the federal electronic verification systems necessary to comply with the law. Only one of the five national electronic systems required to verify identification documents is fully operational, and it will take considerable time and testing for the federal government to update its systems to meet the information requirements of the Act. Require states to employ electronic verification systems only as they become available
- adopt uniform naming conventions to facilitate electronic verification between files as an individual's name is a person's most common identifier, and
- establish card security criteria based on performance—not technology, as limiting states to a single technology configuration increases risks and reduces innovation.

Some of these recommendations are reflected in the NPRM; unfortunately, others are not. Had they all been accepted, significant progress would have been made toward encouraging state compliance with the Act. The Report highlighted four major categories that represented the most critical challenges facing states and customers of DMVs as the Act's implementation deadline approached. The key areas of concern, representing more than \$11 billion in costs over five years, noted that re-enrollment expectations, verification system requirements, card design standards and support requirements placed unreasonable and undue burden on the states. It was also noted that if the implementing regulations were not reasonably crafted, the difficulties of complying with the statute, especially by May 2008, were insurmountable.

Still, many of these same issues ring true based on the requirements of the NPRM. AAMVA, NGA and NCSL are disappointed that many more of its recommendations were not adopted and that our compelling concerns were not acknowledged. DHS has recognized that the cost for implementation of the Act's requirements far exceeds \$11 billion, and more likely represent at least a \$23 billion unfunded federal mandate.

As evidenced by the AAMVA/NCSL/NGA Report, P.L. 109-13 presents significant operational and fiscal challenges to states and the federal government. It also represents considerable impact on individual citizens.

AAMVA members acknowledge that this NPRM is complex and AAMVA members also know that the driver's licensing process is complex. The provisions of this NPRM, however, make the driver's licensing process even more complicated and unnecessarily burdensome. The NPRM's provisions far exceed the development of minimum standards that make practical and operational sense. As well, AAMVA members are concerned that the regulations which have such a massive impact on almost every US citizen over the age of 15, almost every immigrant to the US and every motor vehicle department in every state were not issued until nearly two years after the law was passed by Congress and that little consideration was given to realistically extending implementation and re-enrollment deadlines specified in the Act. States cannot react to this type of mandate with so little planning. Congress and the Department of Homeland Security continue to have unrealistic expectations of states' abilities to implement many of the provisions of the REAL ID Act.

While the NPRM provides some clarification and a degree of flexibility to the states, it continues to cause grave concerns for states and includes provisions that have tremendous impacts on states' abilities to effectively issue driver's licenses and identification cards and fulfill their statutory requirements to their citizen-customers. The NPRM still has vague and onerous requirements that make "operationalizing" the Act very difficult for the states. Many clarifications are still needed, and it is evident that even after ample time to carefully consider the impacts and previous AAMVA member recommendations that this NPRM falls short of making REAL ID "real."

AAMVA members appreciate the willingness of DHS to conduct listening and clarification meetings with the states. It was clear at the four sessions that were held across the country with AAMVA members that the NPRM is a "starting point for dialogue." The NPRM needs to be the most basic starting point and much dialogue is still needed. AAMVA members also appreciate the efforts of DHS to continue to work with AAMVA members to fully understand the impacts and implications of some of the provisions of the NPRM and to better comprehend the real workings of a DMV. These types of discussions are important and AAMVA members continue to be available to provide input and experience to DHS.

Based on the input of our members, our past experience in the area of identification security and the past implementation suggestions that have been presented in numerous venues to DHS, AAMVA members are taking this opportunity to provide recommendations and ideas on how to best accomplish the intent and the concept of the REAL ID Act. AAMVA members strongly believe that the recommendations presented here offer workable solutions to help states which plan to meet the objectives of REAL ID.

AAMVA members encourage DHS to adopt final regulations that incorporate the recommendations of this NPRM response. As well, we urge Congress to appropriate sufficient funds to allow states to implement the statute. AAMVA members also urge the Secretary of the Department of Homeland Security to request funds for REAL ID in the Fiscal Year 2009 Budget request for the agency. States cannot continue to bear the burden of this type of unfunded mandate that drains limited state resources and forces additional costs on its citizens.

To be clear, the driver's licensing and identification card issuance goals of REAL ID are laudable, but only by working together will AAMVA members and the federal government succeed in meeting the challenges

presented by REAL ID. AAMVA's response to the NPRM can assist states in meeting the challenges of the Act and assist DHS in addressing the national security issues that formed the basis for the Act.

AAMVA members have crafted this response to the NPRM to speak to the key overarching concerns of our members in the various categories of the Act. It also is compelled to call out basic foundational issues that not only functionally, but fiscally, impact the ability of states to comply with the statute. Time and money, and lack thereof, continue to drive all the other factors of compliance with the Act and the NPRM. It is expected that states will, on their own, respond to the provisions and concerns of the NPRM from their specific state perspectives. In order to address the concerns of AAMVA's Canadian membership, it is expected that our sister association, the Canadian Council of Motor Transport Administrators (CCMTA), will respond to this NPRM as many of the provisions affect cross border interests. AAMVA members are hopeful that DHS gives thoughtful and deliberate consideration to these responses as all jurisdictions have different implementation issues and unique circumstances.

### **TIMEFRAME FOR IMPLEMENTATION**

The REAL ID Act and this NPRM will have wide-ranging impacts on citizens, state motor vehicle departments, law enforcement, the driver licensing industry and ancillary agencies in state government that rely on and support motor vehicle departments. It will require changes to about 245 million driver's licenses and identification cards, significantly alter state fee structures for license products and change business practices in every motor vehicle department.

This type of massive change cannot be accomplished, and these far reaching impacts cannot be effectively managed, in the timeframes proposed in the NPRM.

Perhaps the best way to comment on the proposed timeframe for implementation and for re-enrollment is to use the words of an AAMVA member who is interested in finding a way to make REAL ID work. "The timeline is a recipe for disaster," he said. That has been the echoing call from all AAMVA members. The timeline proposed in the NPRM for implementation and re-enrollment makes it difficult for any state to even want to attempt to comply. It may, in fact, make it easier for those states that have already voiced concerns not to comply. States have computer system constraints, legislative session constraints, fiscal constraints and procurement constraints that require long lead times for planning and change.

AAMVA/NCSL/NGA indicated in September 2006 that it would not be possible to implement the law by the due dates and that re-enrollment would require at least a 10 year timeframe. An extension to December 31, 2009 is still not enough time for states to comply, and a May 11, 2013 deadline for re-enrollment is just as problematic.

AAMVA members recommend that implementation dates be pushed back, and a second NPRM be issued in July for states to have another opportunity for comment. There are just too many variables to make regulations final this summer without an additional chance for comment. DHS' Verification Systems Task Force is not expected to complete its work until after the NPRM comment period is over, and this is an area that is especially important to AAMVA members. It is anticipated that DHS will receive a firestorm of

criticism in response to this NPRM. Therefore, we strongly recommend that the agency propose again or publish a notice reopening the comment period, and announce new policy options based upon comments on these proposed regulations from the states—who, in the end, will have to implement the final regulations. AAMVA members also recommend that an implementation time not be set until all the required or prioritized verification systems are operational in real time and accessible to all jurisdictions, and that states have at least nine months to connect to the any verification system prior to REAL ID credential issuance.

AAMVA members also recommend that a 10 year, progressive re-enrollment schedule be established beyond the implementation date. The proposed re-enrollment period in the NPRM, effectively three years (2010-2013), is nearly impossible for states to meet since most states have four years or longer renewal cycles.

### **COST**

Implementation of the REAL ID Act is now estimated by DHS to cost at least \$23 billion. Based on the NPRM requirements, this excessive cost is not surprising, but it is concerning.

AAMVA, NGA and NCSL have repeatedly called on the federal government to provide the funds necessary to comply with the REAL ID Act. It is heartening that the NPRM is much more realistic regarding the costs than the initial Congressional Budget Office estimate on the REAL ID Act. While AAMVA members estimated costs to be \$11 billion over five years, that estimate was not based on the specific items in the NPRM, as they were not yet known. The \$11 billion estimate did not account for facility security requirements, the development of federal verification systems and transaction costs, the expansion of the AAMVAnet system to support additional verification connectivity requirements, law enforcement training and technology deployment, expanded public education, data privacy protection and increased customer demand/care and advocacy.

The REAL ID Act National Impact Analysis underestimated the full impact of REAL ID. States are currently looking at cost projections based on the NPRM and reporting increases from their original estimates. Increased costs are expected in card security, physical security, re-enrollment and certification if the regulations stand as proposed.

Past and proposed federal budget submissions by the Department of Homeland Security to Congress and the Office of Management and Budget have fallen far short of securing the funding needed for both the federal government and states to implement REAL ID. The fiscal year 2006 Budget included \$40 million, of which only \$6 million has been allocated for “state pilot” projects. The fiscal year 2007 Budget includes zero funding for states or DHS. Funding must be secured that is reliable and ongoing for the states and DHS. We understand that the fiscal year 2008 Budget also includes no funding for REAL ID. AAMVA members encourage DHS to seek and secure funding for fiscal year 2009, especially for the states to begin implementation of REAL ID. The short term success of REAL ID requires federal funding and the long term success will require ongoing annual, federal appropriations.

The stark reality is that zero federal dollars exist for the states to implement P.L. 109-13. Federal funding is fundamental to implementation of any of the provisions of the REAL ID Act, and the current federal position falls sadly short.

### **AUTHORITY**

AAMVA members remind DHS that many states cannot implement federal laws or regulations without companion or enabling state legislation and in some cases enabling state regulations. States could not begin to consider advancing enabling legislation until the NPRM was published. Even then, states are unlikely to advance legislation based on proposed rules. In many cases, state legislatures are reluctant to simply adopt federal laws by reference. States need at least two years after final rules to adopt the provisions of the statute and will remain very skeptical about completing any work or entering into any contracts until state authorizing legislation is passed. Based on the current state legislative climate and the vigorous opposition to REAL ID in many legislative chambers, it is unrealistic to expect that states could have enabling legislation and/or regulations prior to summer 2009. This reality further exacerbates a January 1, 2010 implementation date and a May 11, 2013 re-enrollment date. DHS needs to recognize these hurdles that the states face.

AAMVA members recognize that DHS has repeatedly noted that states do not have to implement the REAL ID Act and that the only “penalty” would be that the state’s citizens would not be able to use a non-compliant driver’s license or identification card for federal official purposes—such as boarding airplanes. While this is true, even the restrictions surrounding federal official purpose as proposed in the NPRM, put states in a concerning position if they do not implement the Act. States are further constrained on their implementation decisions based on the NPRM’s requirements and provisions for a non-compliant REAL ID credential. The Act permits a state, otherwise in compliance with the Act, to issue driver’s licenses and identification cards that do not conform to the statute’s requirements. However, such driver’s licenses and identification cards cannot be used for an official purpose and must clearly state on the face of the card that a federal agency may not use it for an official purpose. The state also must use a unique design or color indicator so that it is readily apparent to federal agency personnel that the card is not to be accepted for an official purpose. AAMVA members assert that this requirement forces states to be in compliance with other aspects of the Act and that the rulemaking goes well beyond congressional intent in prescriptively outlining state requirements for “non-compliant” REAL ID credentials. The requirement for states to use unique colors for non-compliant credentials is unreasonable and unnecessary unless there is a national standard. The Transportation Security Administration (TSA) cannot expect airport screeners and security personnel at federal facilities to know the color used by each state.

### **DEFINITIONS**

AAMVA members have specific comments on the following definitions outlined in the NPRM. More are anticipated from individual state responses.

1. **Digital Photograph.** The NPRM defines “digital photograph” as “a digitally printed reproduction of the face of the holder of the license or identification card.” AAMVA members believe that this

definition needs to be expanded to include the use of a color image and to allow states flexibility based on their own issuance systems.

2. **Official Purpose.** The NPRM defines “official purpose” as accessing federal facilities, boarding federally-regulated commercial aircraft, and entering nuclear power plants. While the limitations placed on “official purpose” are appreciated by AAMVA members, it is concerning that this definition may be discretionarily expanded by the Secretary of DHS. Except for national security emergencies, the regulations should establish a process for state input should the Secretary decide to expand the scope of this definition. This definition as well could have unintended impacts on commercial drivers who travel intrastate and interstate and require access to nuclear power plants, military establishments and other federal facilities. If states choose not to comply with REAL ID, these drivers could potentially be denied access to these facilities. An alternate form of identification is essential to ensure that commercial carriers and their drivers who deliver to federal facilities continue to have unimpeded access to these facilities, that their livelihood is not impacted and that interstate commerce is not impeded.
3. **Reissued.** The NPRM defines “reissued” as a card that a state DMV issues to replace a card that has been lost, stolen or damaged. This definition needs to be amended to include “only when material changes are required such as name changes.” While some states reissue cards either by statute or at customer requests when addresses have been changed, many do not. DMVs view address changes, in this context, as non-material changes. It recognizes that these changes are important to law enforcement and that they do have access to changes of addresses in DMV databases.
4. **Temporary lawful status.** A person in temporary lawful status is a person who: has a valid non-immigrant status in the United States; has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for lawful permanent resident (LPS) or conditional permanent resident status. The states have noted that this definition still lacks clarity and will result in confusion on the front lines of DMVs. All definitions surrounding lawful presence referred to in this NPRM need to be clearly defined in the final rule. AAMVA members also recommend that a fully functioning and real time Systematic Alien Verification for Entitlements (SAVE) system be the ultimate determination of a customer’s lawful status.

AAMVA members bring to DHS’ attention that the REAL ID statute directs the agency to set standards in consultation with the Secretary of Transportation. In its Medical Certification Requirements for Commercial Driver’s Licenses, US DOT’s Federal Motor Carrier Safety Administration (FMCSA) is proposing new definitions for driver licensing terms. AAMVA members recommend that the consultation intent of the statute be carried out and all definitions relating to driver licensing be synchronized.

## **GRANTS**

AAMVA members are encouraged by the DHS proposed grant application review/approval process for the remaining available \$34 million of dedicated grant funding. It is important that this process also include a

thoughtful review of potentially competing applications to avoid wastefully funding duplicative pilot projects. DHS should also provide guidance to states on tailoring pilots to ensure positive pilot results can eventually be combined with results of other pilots to provide large scale solutions for multiple jurisdictions.

DHS should publicize clear operational priorities and grant criteria that correspond to operationalizing those priorities. For example, funding should be provided to a state to serve as a pass through agency to afford central system development by AAMVA that will benefit all the states in the verification compliance requirement with the state to state and state to federal queries. DHS should also consider funding for states to allow for the deployment of anti-fraud efforts that are currently underway to better secure the licensing process. Many states are currently verifying social security numbers and using photo matching tools to prevent and detect fraud. Grant should be able to be used for these efforts.

While DHS issued a letter from the Office of Grants and Training on March 1, 2007 in the Office of Grants and Training Information Bulletin No. 244 advising states that they could request up to 20 percent of their fiscal year 2007 State Homeland Security Program (SHSP) Funding to help implement REAL ID, this effort does not effectively assist the states in seeking realistic funding for the implementation of the Act. It is AAMVA members' understanding--an understanding confirmed by DHS representatives, that 80 percent of a state's homeland security grants must be passed along to local governments. Therefore, only 20 percent of 20 percent (or 4 percent) of the available grants MAY be used for REAL ID. Recognizing that homeland security grants to states have been reduced in the past few years, and that states have already prioritized this limited grant funding for higher priority projects, there is very little, if any, money available for DMVs through DHS grant funding. Funding for the implementation of this \$23 billion mandate involves basically a zero contribution from the federal government. AAMVA members, governors, state legislators and members of Congress have repeatedly made it clear that the only way many of the provisions of this Act, and its regulations, can be implemented is with full federal funding for implementation and ongoing federal funding to support the added operational costs to states. Realistic funding sources must be identified.

### **MINIMUM ISSUANCE STANDARDS**

This area of the NPRM is foundational to all the other parts of the rule. Therefore, it is one of the areas in which AAMVA members have great interest and concern. This part of the NPRM fundamentally changes the business processes of all DMVs and has significant impact on the nation's 245 million drivers and identification card holders. AAMVA is limiting its comments to key concerns, as it is expected that each state that chooses to respond will verbalize its specific impacts.

#### **§ 37.11 Application and documents the applicant must provide**

AAMVA members are generally supportive of the documents that are suggested to prove identity, date of birth, lawful status and address. As states have improved their issuance processes, they too have limited the documents that can be used for any new issuance.

AAMVA members also generally support a mandatory facial image capture for persons applying for a license. The capture of a digital photograph and signature has become standard best practice among the

states. However, in many cases, photo capture is the last step in the driver's license and identification card issuance process, following the verification of eligibility. Some states also do not capture photos of those denied licensing. A change in the sequence of the photo capture and requiring a photo of those who do not make it through the process can be very costly for states. This direction would require extensive contract changes and require extensive process and facility changes. Such changes require significant programming and database changes and possibly additional equipment, to reflect the change in the business process. As long as a facial image is captured when a credential is issued, and before a credential is denied if a state chooses, states should be provided the flexibility to engineer their system and business processes to best fit their circumstances. Photos should be taken where states believe necessary and changes to the process made only where operationally and physically possible. States should also determine image retention periods for all their images and not be constrained by the NPRM guidance.

AAMVA members are pleased to see that DHS has recognized the sensitivity of licensing in support of law enforcement and criminal justice officers and has provided states with exceptions for this type of confidential processing. While states are not required to comply with the rules when issuing alternative credentials to law enforcement, it is important to note that the success of such programs hinges on the alternate credentialing process being identical to, and indistinguishable from, what is done in the real world. In that regard, DHS should require all state and federal agencies issuing REAL ID approved source documents (vital records, Social Security Administration, DHS, DOS, etc.) to also implement procedures whereby local, state, and federal law enforcement personnel may obtain those source documents with the alternative information, and that the issuing agencies develop processes whereby state DMVs can verify the issuance, validity, and completeness of the documents and information, just as if they were legitimate verification inquiries. The Social Security Administration has developed such a process. In other words, the alternative or special licensing verification process should mirror the requirements of Section 202(c)(3)(A) of the Act. Further, the agency providing the verification should develop procedures to insure the inquiry and response appear legitimate, even to their own employees.

AAMVA members also point out that some states have indicated that there is not a need for the presentation of the Social Security Card as required in Section (e). With electronic verification, states should have the flexibility to require the card or not.

Ineligibility for a Social Security Number must be identified to the states by a formal, secure document or electronic system indication issued by the Social Security Administration or SAVE and supported by stringent rules and policies applied consistently to ensure accurate representation. After discussions with DHS, Social Security Administration and Systematic Alien Verification for Entitlements System (SAVE) representatives, there is an indication that there may not be a way to effectively determine ineligibility and that this provision may be a statutory requirement that is not possible to meet. As this is an issue for DMVs, AAMVA members recommend that further discussions be held to find an alternative to meet the intent of this provision.

AAMVA members also recommend that DHS consider the use of an expired passport as an acceptable identity document. As the passport is one of the more secure identity document used for driver's license and identification card issuance, some states allow this now.

There is one other concerning matter in this section involving the exception processing for applicant documents and reporting on exceptions to DHS. All states currently operate with exceptions processing. They understand the need to document the exception made and who made it. However, it is unrealistic to expect the DMVs exception process to be approved by DHS and for DHS to take the time to do so. There are literally hundreds of "exception" scenarios. This "approval process" is too far into the day to day operational aspects of the business for DHS to reach. It is also unrealistic to expect a state to provide DHS with quarterly reports analyzing the exceptions process. This is a costly administrative undertaking. And finally in this section, states routinely document any exceptions with the application. It is not feasible for states to mark the exception on their data files until such time as they complete computer system upgrades.

### **37.17 Requirements for the face of the driver's license or identification card**

The requirements outlined in the NPRM are fairly consistent with the AAMVA *Driver Licensing/Identification Card Design Specification*. However, one of the basic underlying requirements of this provision causes concern for AAMVA's members: full legal name.

**Full Legal Name:** There is wide inconsistency as to how agencies which issue identification credentials document a person's full legal name. There is a need for acceptable common business practices among issuing agencies on what is captured on the face of the document, included in the machine readable zone (MRZ), as well as a hierarchy of use when inconsistent documentation is presented by applicants. Documents such as passports, immigration documents, social security cards and birth certificates have disparate names. This is most concerning with federal documents, as there is no standard naming convention for federal agencies. The federal government is inconsistent in its application of full legal name, thus putting states in a reactive position with customers. This is a large security loophole at the federal level. The federal government has not recognized this important underlying component in their issuance systems, especially with passports. US passports, used as breeder documents for REAL ID credentials, makes the name matching difficult and results in many issues for customers whose names on passports do not match birth certificates or marriage certificates. The requirements for obtaining a passport are substantially less rigorous than those proposed for a REAL ID credential. The same is true with the Social Security Administration and social security cards. AAMVA members implore the federal government to move toward a standard convention for full legal name on the issuance of any federal government document. DMV front line employees are constantly confronted with putting the links in the naming chain together, and a lack of a federal naming convention makes this difficult now with social security number verification and will make it doubly difficult with passport verification and immigration verification for foreign names.

One of the basic underlying ways of ensuring one driver, one record rests in the name. Federal agencies must complement state efforts in this fundamental aspect by capturing and retaining full legal name consistently so that DMVs are able to verify full legal name with issuing agencies databases.

In the absence of a consistent use of full legal name by federal agencies, DMVs should be able to use their own processes and procedures, based on documents provided by the applicant, to determine the name that is put on a driver's license or identification card and the information that is retained in the state driver

licensing system. Considerable state flexibility is needed here and DHS needs to alter the definition of full legal name and the requirements under §37.17 (a) to allow states to continue to make their own determinations, based on documents presented, to determine the name on the driver's license or identification card. As well, the barring of initials or nicknames needs to be stricken from the NPRM. To emphasize the reality of conforming to this type of requirement, one state recently attempted to transition from "known" names used on driver's licenses and identification cards to "full legal name" and had significant legal and customer issues with this approach. Customers who used "known" names for many years on their credentials were deemed legally able to continue to use the "known" name and issues at DMV counters significantly increased. These issues forced the DMV to relax this direction. This state's experience is indicative of issues that would be exacerbated nationwide if the NPRM definition of full legal name stands. DMVs cannot be expected to adhere to this standard as long as the issuers of all major federal identification credentials do not adhere to the same naming convention.

Additional clarification is needed from DHS in defining the processes for handling different naming conventions and cultural differences in naming conventions.

Naming conventions in general are concerning to AAMVA's members. Beyond the name and "nickname" issues, considerable work needs to be done with foreign names and cultural names. AAMVA members have done work in name collection, use and maintenance and have provided guidelines to states as part of the *Driver's License/Identification Card Security Framework* and the *Driver License Agreement*. Truncation guidelines should also be developed with input from states and applied to all systems used for REAL ID verification. As it relates to the credential, DHS should follow the *AAMVA Driver Licensing/Identification Card Design Specification*.

**Address of Principal Residence:** While many states use address of principal residence, except for confidential issuances, some currently do not require applicants to include their address of principal residence on the face of their driver's license or identification card. The NPRM is very restrictive as to when an alternative address, other than address of principal residence, can be used. State statutes also vary widely on the interpretation of address of principal residence. It will be difficult for states to abide by one standard definition as outlined in the NPRM. States should have the flexibility to utilize an alternate mailing address on the driver's license and identification card as long as the address of principal residence is captured and maintained in the driver licensing database.

This rule also requires that the iris and pupil of the eyes shall be clearly visible in the full facial digital photograph. Because this requirement may require some states to purchase new camera equipment, we believe DHS should provide further justification about the reasons for this requirement and whether they intend to add a biometric element in the future. AAMVA members clearly need to understand DHS' intentions with this direction as biometrics will have more significant impacts not yet explored.

### **§ 37.19 Machine readable technology on the driver's license or identification card**

Many of the provisions in this section of the NPRM basically follow the Machine Readable Technology (MRT) requirements of the *AAMVA Driver Licensing/Identification Card Design Specification*. Most

states are currently using or moving toward the PDF417 standard as contracts come up for renewal or re-bid. AAMVA members are supportive of all the requirements noted in the NPRM for the machine readable portion of the REAL ID compliant driver's license or identification card, with the exception of the mandatory requirements of full name history and name changes. These should be optional elements for states. AAMVA members recommend that the only mandatory minimum requirements for the MRT be those noted in the *AAMVA Driver Licensing/Identification Card Design Specification*.

Encryption is an area where AAMVA members, and especially its law enforcement members, have concerns. The information/data carried in the common MRZ is the same information/data that is human-readable on the driver's license or identification card. There are a number of good reasons for leaving it this way. A principal argument against encryption is the automation benefit that having access to the information has afforded DMVs and law enforcement in their line of duty. Being able to access the information/data is critical to current and future projects that provide interoperability within this community. Whether it is a customer visiting their local DMV office or a police officer completing a citation/report, that process is greatly enhanced by allowing for the information/data to be read and verified. Were there to be a problem with having access to the decryption key, if the information/data on the credential was encrypted, then obviously this would have a tremendous impact on those processes. There too are economic challenges of rolling out an encryption methodology and infrastructure that go well beyond the REAL ID Act. Key management is a huge concern. There would be the ongoing cost and administration of distributing and protecting the key(s) used for encryption/decryption. The encryption key(s) would eventually be compromised and released to the general public, rendering them useless. Changing keys would be costly and would not protect existing encrypted credentials.

Attention needs to be focused on the misuse of the information on the card either by photocopying or writing it down from the front of the card or swiping it through a "reader." Increased attention is necessary in the states and by the federal government limiting the access and use of this information. AAMVA members have recognized the need to address privacy concerns with the MRZ. In its *Driver's License/Identification Card Security Framework*, AAMVA has recommended that all jurisdictions consider legislation limiting the use of information collected and used from the machine-readable portion(s) of a driver's license and identification card.

Besides law enforcement, there are many other authorized users of the driver's license and identification card, including DMVs. Encrypting the information denies many of these users, such as banks and retailers, the ability to ensure that the human readable information on the front of the card matches what is carried in the MRZ. Fraudulent credentials have been uncovered in this manner, and encryption literally denies this measure of security. Encryption does not provide the benefits those outside the motor vehicle community believe it does.

As law enforcement is a major user of the MRZ and many forces have invested funds in readers, encryption impedes this investment and time-saving process and could potentially undermine the states' efforts to efficiently collect conviction data in a timely manner especially for programs monitored by the FMCSA. AAMVA members do not support any encryption efforts on the driver's license or identification card.

### **§ 37.23 Renewed and reissued driver's licenses and identification cards**

This area of the NPRM is very concerning to AAMVA members. As noted, the timeframe for re-enrolling all customers by May 11, 2013, is extremely problematic for states. Proposed state procedures outlined in the NPRM to establish confirmation of the applicant's identity each time a REAL ID credential is renewed or reissued are wasteful and burdensome requirements that are not necessary. For example, if the social security number and passport information is verified once, there is no need to re-verify it as the basic information is unlikely to change. Many states already require in-person visits to complete name changes. As well, states are currently in the process of deploying photo matching prior to renewal or replacement and many states that are over-the-counter issuing jurisdictions confirm social security numbers and photos prior to issuing a renewed or replaced credential. States also are required to check the US DOT National Driver Register's (NDR) Problem Driver Pointer System (PDPS) prior to renewal or replacement. Many states will mark their system records as confirmed verifications. Completing these steps at time of renewal or replacement is a waste of time, energy and money.

The requirement to re-verify source documents at each renewal and any time any information has changed significantly impacts the automation and effective technology and process improvements states have put in place. The specific requirement to re-verify source documents such as address documentation is not possible to meet as there is no electronic system to do so. The requirement to demand in-person renewals any time any information changes, such as address, is flat out ridiculous and unworkable. Address changes are one of the most frequent record changes done by states. Highly automated and effective methods, such as telephone, mail and internet renewals, are used to accomplish these high volume transactions which total well over a million transactions a year for larger states. Security is about the identity, not an address change or a passport expiration date.

In-person renewals are also problematic. Some states have four-year renewal cycles, and an every other in-person renewal cycle would require customers to visit the DMV every eight years versus the NPRM requirement of every 16 years. States with shorter renewal cycles are penalized. Many states also require photos to be taken at every renewal cycle. Renewal cycles in states are ancillary to the REAL ID Act and only critical for re-enrollment. States should be able to continue to determine renewal length based on their business processes and business needs.

Renewals and replacements due to lost products are a large part of the DMV business and the processes surrounding them are highly automated and technologically advanced to allow for operational effectiveness and customer need. Changing any processes surrounding renewals or replacements has the greatest impact on the states and results in the least impact on national security. The risk does not warrant the draconian measures contemplated in the NPRM. DHS should view this measure from a risk/value proposition. AAMVA members contend that the risk is low and the value is minimal.

In an effort to improve service and reduce costs, motor vehicle agencies have increasingly taken advantage of technology and the use of alternative service channels to handle driver's license and identification card renewals by telephone, mail and the internet. The popularity and success of these channels have now grown to handle as much as double-digit percentages of renewals in some jurisdictions. Loss of alternative

channel renewal opportunities will be expensive and have significant adverse impacts as counter personnel will be insufficient to handle the increased traffic and the added vetting requirements of the NPRM. The result will be significantly more crowded offices and longer wait times; not necessarily improved national security.

AAMVA members are supportive of in-person renewals for temporary REAL ID driver's licenses or identification cards, as these are limited time documents and lawful status can change. This segment of the customer base is far fewer and the process surrounding this issuance is much easier to manage with in-person renewals than the larger US citizen population. AAMVA members recommend that this section of the NPRM be entirely stricken with the exception of (B)(2)(iii).

To be clear, AAMVA members recommend that only material changes, like name changes, be considered if any in-person renewals or replacements are required and that states be able to design a renewal and replacement strategy that meets the needs of each state. AAMVA members also recommend that DHS:

- Allow states to determine if they want to re-vet or not. Once a REAL ID credential is issued, and the customer moves, the new state of residency should be able to determine what re-vetting they believe is necessary.
- Allow states to continue alternative renewal channels and continue to use the verification channels they use now prior to issuing a renewal notice (social security number on-line verification, image verification, Commercial Driver License Information System (CDLIS) verification, PDPS verification and any other verification systems they currently have in place).
- Allow the DMV to renew a previously issued REAL ID compliant driver's license or identification card through mail or internet.
- Allow holders of REAL ID compliant driver's licenses and identification cards non in-person change of address during the license validity period without the required issuance of a new credential document unless a state statute requires it.

As this area is such an important issue and a potential "show stopper" for many states, AAMVA members reiterate that it is wasteful, ineffective and inefficient to require customers to visit the DMV when non-material changes need to be made to their driver's license or identification card. Many states do not require the customer to get a new credential for an address change. Customers and DMVs are also able to avoid the added cost. States need to continue to set their own renewal and replacement issuance and verification standards.

The resultant effect of this section is the taking of many steps backwards for DMVs and the technologies they have deployed. These technologies have reduced costs to both customers and the business. The provisions of the NPRM, as they relate to renewals and re-enrollment, revert states to antiquated, time-consuming and costly processes with little contribution to protecting homeland security. Again, DHS should consider re-enrollment from a risk/value perspective.

## **PRIVACY REQUIREMENTS**

AAMVA members recognize the importance of privacy and confidentiality of information and the protection of customer information in all forms of use, access and dissemination. Many states have privacy laws that are more restrictive than the Drivers Privacy Protection Act (DPPA). AAMVA members will continue to work with DHS on ensuring privacy, and are more than willing and prepared to provide specifics on privacy protection in their security plans provided to DHS. AAMVA members remain very interested in the “federal reference” databases and will continue to provide input to DHS on the development, governance and protection of the data and information in those databases. DHS has yet to provide specific information on how this “query” system will work and does not expect to provide that information until the comment period is over. This is another reason why AAMVA members believe that final rulemaking should not take place until there is opportunity for another round of comments. Once again this direction is only feasible if all dates for implementation are pushed out.

Clearly, states are concerned with access required for verification of federal information such as social security number, immigration status and passport information. As well, they are clearly interested in the access and use of information contained in their own systems. It is anticipated that any “all-driver” system would work like the current CDLIS; for which there have been no data breach or privacy and confidentiality issues.

AAMVA members are more than willing to work directly with DHS on these systems and privacy issues and implications. As part of its *Driver's License/Identification Card Security Framework*, AAMVA has recognized the importance of privacy and put forth the following eight Privacy Principles for states to consider:

1. Openness: Each DMV shall inform the public of all systems and databases that are being established or have been established for use in driver's license and identification card issuance; the public shall be informed of the nature of the information systems that are maintained and used for the purposes of administration of the laws that pertain to the licensing of drivers.
2. Individual participation: Each individual has the right to examine the data kept on himself/herself by the DMV and request the making of corrections to that data.
3. Collection limitation: Each DMV shall have a clear list of required personal data elements.
4. Data quality: Each DMV shall ensure that all data is “accurate, complete, current and verified.”
5. Use limitation: Each DMV shall specify how it uses personal information and shall adhere to this specification.
6. Disclosure limitation: Each DMV shall adhere to a specified disclosure limitation that indicates what personal information may be disclosed and how it may be disclosed.

7. Security: Each DMV should protect all data kept.
8. Accountability: Each DMV shall ensure it has a means to oversee and enforce the previously mentioned principles.

As proposed in the NPRM, each state is required to submit, as part of the REAL ID Act certification process, a written comprehensive, security plan. States are prepared to address privacy in their comprehensive security plans and, in fact, many states already have these types of plans and procedures in place. Privacy and confidentiality concerns are not a new issue to state DMVs, nor are their application. AAMVA members also recommend that DHS continue to emphasize AAMVA's member developed model legislation to prohibit the capture and storage of personal information obtained from a driver's license or identification card as DHS' Privacy Office has referenced in the Privacy Impact Assessment. It is also recommended that DHS work with Congress on strengthening the Drivers Privacy Protection Act.

### **IMMIGRATION REQUIREMENTS AND TEMPORARY DRIVER'S LICENSE AND IDENTIFICATION CARDS**

#### **§ 37.21 Temporary driver's licenses and identification cards**

Some of AAMVA's member states continue to support the issuance of driver's licenses and identification cards to non-US citizens who are not lawfully present in the United States.

Many states have already moved to improve how they license and identify non-US citizens. Much progress has been made in changing processes and in securing legislation for limited licenses and end of stay expiration. Most states too have adopted lawful presence laws. However, those states that have not done so will need time to pass legislation to require lawful presence for the issuance of a REAL ID-compliant driver's license or identification card, synchronize the driver's license and identification card expiration date with the authorized end-of-stay date and train employees to verify lawful presence. AAMVA members have consistently opposed the "branding" of a temporary driver's license on the front of the license for non-US citizens. The minimum requirement for identifying restricted driver's licenses and identification cards duration should be indicated as a restriction code on the front of the credential, with clarifying language on back. This is standard for other license restrictions. This recommendation will also reduce additional cost impact to states.

It is recognized that states must verify the immigration documents an individual presents to establish his or her temporary lawful status through the SAVE system. The use of an electronic verification system is really the only way to determine lawful status. There are, however, inherent issues with SAVE that must be addressed before it is deployed nationwide and states are required to use it. This system, while closer than some, still needs considerable work to ensure its reliability and functionality and to reduce impacts on the DMV. AAMVA members recommend the following actions as they relate to the SAVE system: responses to SAVE inquiries should consistently include the appropriate end-of-stay date for capture on the driver's license and identification card, limit document verification to what can be accomplished through an enhanced SAVE program that is fully developed, operational in real-time and accessible to all jurisdictions

at no cost to states, SAVE operability must allow for reliable real-time response in a high-volume hub-based query environment, which can be integrated into DMV transaction processes, and the AAMVAnet system similar to the Social Security Online Verification System (SSOLV). SAVE should be considered a priority for the verification systems development schedule.

States will be unable to comply with the expanded mandatory use of the SAVE system without funding, full development, functionality and accessibility. While immigration document training of DMV counter service personnel has progressed in the past few years, an electronic and reliable verification system is essential for DMVs to determine immigration status and lawful presence. SAVE will not work if its information is not current, if secondary responses are the norm versus the exception and if it cannot be integrated into already established state verification systems. AAMVA engaged its members in a working group to lay out the systems and business requirements for SAVE and would be happy to work with DHS on specific requirements to make the SAVE system meet our members needs. DHS should establish a state working group to ensure the appropriate functionality of the SAVE system for the purposes of this Act. With or without REAL ID, the SAVE System, if functioning at optimal capacity, is a vital verification tool for states.

As it stands now, SAVE currently lacks the real-time functionality to provide truly integrated verification for the full range of non-US citizen applicants in all DMVs simultaneously. SAVE also requires escalation of cases through a manual process which can currently require days or weeks to resolve, even at its limited current usage by only a few states. Internet access is rarely practical in a high-volume, time-sensitive transaction environment, and real-time bridge connections would be required to allow the integration of the SAVE verification into the motor vehicle agency workflow. A mandatory requirement for use of SAVE under P.L. 109-13 requires significant added functionality to the SAVE system which will be subject to high volume transaction demand. AAMVA members have consistently voiced their expectation to also integrate the SAVE System into the AAMVAnet network for ease of operations.

## **VERIFICATION OF DOCUMENTS**

### **§ 37.13 Document verification requirements**

AAMVA members recommend that DHS view the verification requirements in the REAL ID Act and the corresponding NPRM from a risk and value perspective. Recognizing that verification of documents is a verification that the piece of paper is legitimate and not that the customer is the owner of the piece of paper, it is important that risk and value of these systems be carefully considered and that this proposition be considered in prioritizing verification system development for the systems required by the Act.

AAMVA members support the need to electronically verify documents that are presented for driver's license and identification card issuance based on the value that the verification provides. Many of the issues surrounding driver's license fraud and abuse are the result of counterfeit or fraudulent breeder documents. In its *Driver's License/Identification Card Security Framework*, AAMVA points out that wherever possible, all jurisdictions shall electronically verify the data elements required for driver's license or identification card issuance with the originator of those data elements. Almost all jurisdictions now use the SSOLV

system. AAMVA members are interested in getting additional support from the federal government in the remaining required electronic verification systems as some are critical to the DMV business. However, the entire verification area is vexing and the NPRM is concerning on a number of levels. Time and money top the list along with system development and deployment. The concerns and deficiencies pointed out in the previous discussion of SAVE should also be taken into consideration in the development of other verification systems.

In the REAL ID Act National Impact Analysis, AAMVA/NCSL/NGA noted that confirming the validity of an identification document with the issuing agency will be one of the most expensive requirements of REAL ID. Verification processes comprised the second largest category influencing REAL ID implementation costs, accounting for approximately 12.8 percent of the \$11 billion known costs—or a total of \$1.42 billion over five years. The largest contributing factor is the more than 2.1 million computer programming hours states will need to adapt their systems for new requirements involving eligibility verification, business process re-engineering, photo capture and database design. Because DMVs will need to verify at least three identification documents for each applicant, states can anticipate processing more than 1 billion verification transactions over the next five years. Other verification costs include one-time costs primarily related to states establishing connections with verification systems once they are made available and anticipated ongoing operational costs during a previously assumed five-year re-enrollment period. These estimates do not include transaction fees that may be required for states to access these systems or the cost of developing and maintaining the required information systems.

The primary objective of verification and interoperability as viewed by AAMVA members is to reduce the likelihood of driver's license and identification card fraud. AAMVA members support this objective and recommend that the final rules regarding verification be outcome and performance based and recognize the value and risk of the verification requirements as well as the impact on spending resources on systems that may not yield the highest value or potential fraud reduction. AAMVA members recommend that seven basic tenets be considered by DHS as these verification systems are considered prior to final rulemaking. The tenets include:

1. Privacy and security of any personal information is paramount and must be an overriding guiding principle in any system development and use.
2. Any verification system development must minimize the effect on state DMV processes and must be integrated into the AAMVAnet infrastructure--an infrastructure that states use now for connectivity to existing verification programs and requirements such as SSOLV, CDLIS, PDPS and the National Motor Vehicle Title Information System (NMVTIS). AAMVA members emphasize that states do not now and cannot in the future use verification systems that require the input of different names on different documents for individual system queries. This would result in significant front line service issues, employee training issues and computer system issues. The integration into a "one-call" system through AAMVAnet is critical.
3. AAMVA members understand DHS' use of the term "federated" not to include any wholesale database or data access and also understand that the term relates to an information technology

structure that would provide “portal” access for states similar to what states now use with AAMVAnet to access SSOLV, CDLIS, PDPS and NMVTIS.

4. AAMVA members assert that any cost or development of any system be borne by the federal government to meet this federal requirement.
5. DHS should focus on verification systems that have the highest impact and the best value for DMVs to address abuse and fraud in the driver licensing and identification card issuance systems. Currently, high value verification tools exist that can and do reduce the likelihood of fraud--tools that many states are using in the data verification, document authentication and identity assurance areas. Tools such as social security number verification through SSOLV, immigration status verification through SAVE, document authentication through machine verification, document authentication through inspection and photo matching verification are all in use today in many DMVs and are yielding results. DHS should provide the flexibility to states to continue to use these types of tools to meet compliance and certification for REAL ID and should recognize that this direction is an area that yields high fraud detection and reduction results.
6. AAMVA members recommend that DHS view the implementation of verification systems required under the Act through a phased and flexible approach recognizing that some systems like SSOLV and SAVE and tools such as AAMVA’s Digital Image Exchange have the highest value and risk mitigation. DHS should also recognize that proposed verification systems such as the passport verification system have little risk mitigation value and that there are other ways to achieve any value that may be obtained by a full scale and costly birth certificate verification system. AAMVA members assert that there are ways to achieve the mitigation of the fraudulent use of documents through various alternative verification and authentication channels aside from the immediate development of all the five verification systems required in the NPRM.
7. Re-enrollment verification must be left up to states based upon their own individual processes, computer system capabilities and issuance systems as well as their own knowledge of risk mitigation and fraud prevention and detection. As noted in other areas of this response to the NPRM, customers should be “grandfathered in” and re-enrolled automatically if they have been licensed or have had an identification card for 10 consecutive years in a state, if their social security numbers have been verified in SSOLV and their image has been verified. The Final Rule needs to be flexible enough to allow states to be able to make re-enrollment decisions that meet their particular circumstances.

AAMVA members’ compliance with the proposed verification requirement is contingent on the completion and implementation of at least five national identity verification systems and the necessary time for states to complete the required systems integration, process changes and train staff. Compounding these efforts will be the need to comply with state and federal procurement requirements, system security measures and data privacy laws as well as extensive testing associated with the roll-out of any new system. AAMVA members, again recognizing that verification is important in many areas, believe that some of the

verification objectives of the NPRM can be achieved without the immediate requirement for states to connect to some of these costly systems.

AAMVA members' initial recommendations in the area of verification remain consistent and include: the prohibition of federal agencies from charging transaction fees to the states for the required electronic verification of federal information; the establishment of a cooperative effort between the DMVs and the National Association for Public Health Statistics and Information Systems (NAPHSIS); the need for state vital records agencies to provide reliable data and acceptable fees related to the verification of birth, marriage, divorce and death information; the compliance allowance for the states to be required to employ electronic verification systems only as they become available; and the consolidation and synchronization of system development schedules in a cooperative effort to maximize resources, ensure system efficiency and minimize the impact on state and federal systems.

The entire verification infrastructure needs careful consideration. It is understood and noted in the NPRM, that the federal government does not want to manage the verification "middleware" nor does it want to govern system use. Considerable discussion with the states is needed and much effort remains to fully understand DHS' intent here. AAMVA members understand that DHS has a task force looking into the verification systems, but their work will not be completed until after the comment period has ended. This is very concerning as the states must have the ability to comment on verification system infrastructure that is fundamental to compliance considerations. Recent discussions with DHS reveal that a willingness does exist to work closely with AAMVA members on the prioritization, value and use of the verification systems and a willingness to understand the constraints, challenges and tools that states are currently using to verify documents and combat fraud. A continuing dialogue with AAMVA members regarding the verification systems required in the Act is essential.

As noted, REAL ID calls for the use of five electronic verification systems. Only one (the Social Security Online Verification system – SSOLV) is in place and functioning for use in a DMV environment. AAMVA members offer the following additional comments on the various verification systems and the requirements outlined in the NPRM.

**Birth certificate verification through Electronic Verification of Vital Events (EVVE).** It is clear that this system is nowhere near ready for implementation. While DHS is working with NAPHSIS, it is anticipated that there is not enough time to develop the system, for states to connect and test the system and for states to effectively integrate this system into their operating environments. The vague notation that DHS will approve an "alternative system" until EVVE is ready is also concerning to AAMVA members. AAMVA members are hopeful that DHS will work with states to determine requirements and realities of this system as well as its prioritization. AAMVA members recommend that the SSOLV system be used to validate birth in the absence of this system's full functionality and that death records are an even more vital part of any effort to combat driver's license or identification fraud. Again, states should not have to pay a transaction fee to validate information required for this federal mandate. The transactional costs of this system are expected to be well above the few cents per transaction states now pay for SSOLV. These are high volume transactions and will significantly impact state budgets. While this verification system may be a long term answer to continue to address document fraud, there are steps that can be taken in the interim to

achieve some of the same results without a costly near term investment. DHS should work with the Social Security Administration to determine if the current SSOLV verification system can include place of birth information. AAMVA members also point out to DHS that some states already verify or plan to verify birth records of applicants with their own state vital records agencies prior to driver's license or identification card issuance and that an overall birth certificate verification system will only be effective if all states subscribe and that data is accurate. AAMVA members are not aware of any definite schedule or requirement for state vital agencies to subscribe to this system.

**Passport verification through Department of State.** This system is not yet operational and its development and integration into the DMV environment is questionable and concerning. AAMVA members view passports as one of the more secure documents presented to DMVs for driver's license and identification card issuance and some states currently use document authentication tools to authenticate US passports. Therefore, AAMVA members question the value and the risk mitigation of this type of system as compared to the cost of development for the federal government and the states. Since the passport application process does not require the use of "full legal name" it will be difficult for states to determine name matches and therefore the development of this system requires AAMVA members' full participation. Implementation of P.L. 109-13 would require the Department of State to define the requirements of this system, construct the system, test the system and work with AAMVA members to make it available for deployment. It is questionable that this system will be ready for states to comply with the May 11, 2008 deadline or the extended deadline of December 31, 2009. Loopholes in this verification system should be pointed out as a non-compliant driver's license can be used as proof of identity to secure a passport and then the passport can be used to obtain a REAL ID compliant credential. DMVs question this logic. Business requirements in use by federal agencies and their contractors, charged with providing verification services, should never be less stringent than those imposed on the states. This is one of the verification systems that if developed should be assigned a very low priority and is one of low risk/low value in an overall risk/value proposition.

**Immigration document verification through SAVE.** AAMVA members' concerns with this system are previously noted but it must be emphasized that the Final Rule should provide for a contingency if SAVE becomes overwhelmed and does not perform. States will be putting high volumes of verification transactions through the system, especially during re-enrollment. An online, web-based system that cannot be integrated into DMV processing, and does not have batch capabilities, will not work in the DMV environment. It is essential that verification be completed at "first pass." States and customers cannot afford the return visits or the second or third level verifications. They are manual, time-consuming, cumbersome and expensive. If the applicant does not pass the initial verification or in rare cases a secondary verification, they should be referred to DHS/USCIS for resolution. While some states are using this system, its capacity and functionality need to be improved to be effective in the DMV environment. AAMVA members recently were advised that the SAVE System is slated to undergo improvements and that DHS is committed to work with the states to achieve improved functionality and reliability of SAVE and reduced matching and secondary query issues. This is good news and AAMVA members are more than willing to work closely with SAVE representatives as the SAVE system is vital to driver's license and identification card issuance. The improvements to this system should be considered high priority by DHS. AAMVA members also point out again that there are very real concerns with the current cost of the system

and even greater concerns with the proposed cost of the SAVE System. AAMVA members were recently made aware that a fee study was conducted for the SAVE System and that as of October 1, 2007, the SAVE System is required to be self sufficient. SAVE System representatives have advised AAMVA members that costs will materially increase to use the system. AAMVA members are opposed to and concerned with any increase in fees for this system as fee increases will significantly impact state costs and state budgets. This is especially true for states that service many non-US citizens and have high volumes of SAVE transactions. AAMVA members have recommended that federal agencies should be prohibited from charging transaction fees to the states for the required electronic verification of federal information especially if required by a federal mandate.

**REAL ID licenses and identification cards verified with the state of issuance.** Except for commercial drivers, states can now only check with the prior state or states of record to determine the status of a non-commercial driver's license. For this requirement to be implemented, an all-driver system is necessary. This verification system also does not exist and is not expected to in time for a December 31, 2009 deadline. The states must be involved, along with AAMVA, in a system development effort of this magnitude. AAMVA members recommend that the scope of the Congressionally authorized and funded CDLIS modernization project be expanded to include the development of an all-driver system.

**Social security number on-line verification through SSOLV.** Currently 46 states and the District of Columbia have the ability to verify applicants' social security numbers with the Social Security Administration. As states have been using the SSOLV system for some time, they are keenly aware of the technical and operational issues the system presents in a day to day environment. These issues have been communicated to the Social Security Administration and AAMVA members are hopeful they will be addressed. Downtimes are unacceptable and maintenance schedules must continue to be coordinated with AAMVA. One of the positive aspects of this system is that it is integrated into the AAMVAnet network and states can more easily access the system, audit its use and tie it into their back-end operating systems. States have determined that this model, using AAMVAnet should be the integration model for all other systems. As name and full legal name are critical to the identification process, SSOLV too should allow verification of the social security number through the applicant's former name where proof of legal name change has been presented to the DMV.

**Address of principal residence with a system of document verification acceptable to DHS.** This verification system direction emphasizes AAMVA members' continued concerns with lack of clarity in this NPRM. As it has been established, there is no easy way to verify address of principal residence and there is no feasible way to develop or implement an electronic verification system for proof of principal residence, nor is there a compelling security reason to do so. AAMVA members appreciate the consideration DHS has given to using address documents as "verification" of address of principal residence. Many states already use these documents. In order for the states to support this verification concept, additional clarity is needed as to what a "system of document verification acceptable to DHS" really means in the address verification area. AAMVA members recommend that this verification be left to the states to determine and provide DHS in their certification plans.

AAMVA has established a number of working groups of members to assess all of the verification systems required and urges DHS to continue to work with AAMVA's members on determining the requirements of these systems.

It is AAMVA members' expectations that states will not have to "back track" and complete verifications with any system that is not yet operational if they begin REAL ID implementation prior to any system availability. All systems should be "date forward." AAMVA members also expect the verification systems to be one-way and used for the sole purpose of verification. Federal system owners will not be permitted to query state databases.

Verification should be a one-time process. Aside from verifying address or immigration documents, once a REAL ID credential is issued, customers should not have to present these documents when they move to another state. DHS must keep in mind that the DMV environment can only accommodate highly automated electronic verification systems that are reliable; fast; provide real time, accurate information; and are integrated into the driver's license/identification card issuance process.

It is clear that new verification systems will not be up and running in time for a May 11, 2008 implementation. It is highly unlikely they will be functioning and connected to DMVs by January 1, 2010. The verification area is fundamental to improving driver's license and identification card issuance and AAMVA members believe that any implementation date for REAL ID must be tied to the full completion and availability of these core systems or a prioritized implementation schedule with specific outcomes. AAMVA members are more than willing to work with DHS on a prioritization schedule based on risk mitigation and value of investment for these systems. AAMVA members are in the process of developing a recommended phased implementation plan based on risk and value of these verification systems and will share that recommendation with DHS in a supplemental response to the NPRM.

## **INTEROPERABILITY**

### **§ 37.33 Database connectivity with other States**

States have been working toward driver licensing interoperability for many years. The partnership AAMVA and its members have with the US DOT has helped advance interoperability for commercial driver licensing through the CDLIS and has conceptually advanced an all-driver system known as DRIVeRS (the Driver Record Information Verification System). These concepts are fundamental to highway safety and the *Driver License Agreement* interstate compact among states. No all-driver system exists and therefore no database connectivity with other states, as proposed under this section of the NPRM, is possible.

Until an all-driver system is fully developed, operational in real time and accessible to all states (with funding provided by the federal government) the concept of ensuring that a person does not have another license or identification card in any other jurisdiction is impossible, and this interoperability requirement is moot. It is possible for states to verify with the prior state or states of record completing a "state to state" check (and many do), but an all national check and the systems to support those checks are far from a

reality. It will take considerable effort and funds to get there. Until a national all-driver system is federally funded and available, AAMVA members have recommended that states continue to use CDLIS to query if a commercial drivers license exists. They do this now for all commercial and non-commercial drivers as required by the Motor Carrier Safety Improvement Act (MCSIA). States can also require applicants to self-declare the existence of prior licenses and identification cards and require their confiscation and notification to cancel to the prior state upon the issuance of a new document. Many states also do this presently.

Other AAMVA member recommendations for an all-driver system are:

- access to state information is defined as query and response, not wholesale penetration;
- any access must adhere to the DPPA and more restrictive state record confidentiality laws; and,
- access and use are limited to driver's license and identification card issuance and law enforcement management.

It is AAMVA members' recommendation that when a licensed driver or identification card holder moves to a new state, the record will be transferred to the new state. Minimum information will be retained by the former state based on its laws and practices and in accordance with the DPPA. This is the ideal system. But, AAMVA members remain interested in working with DHS to develop alternate solutions to ensuring one driver, one record for all driver's licenses and identification cards.

More specific concerns here relate to control, access and record specificity requirements in the NPRM. The requirements for a system of this type cannot be laid out in an NPRM. They take interaction with the states and AAMVA. States need to determine among themselves what information will or should be included in an all-driver database, what will be available for state inquiries and, what transfer of information should occur. Even the number of characters required to be retained in a database is an example of the need for discussion between AAMVA members and DHS. AAMVA members view the 125 character requirement as the total number of characters to be used for the full name, not just the last name. Any AKA (also known as) names will need to be contained in another data field of 125 characters. This is just one example of why the NPRM cannot serve as the requirements manual for a data system of this magnitude, and its provisions are premature and prescriptive. Again, AAMVA members are willing to work closely with DHS in determining the purpose, use and design of this verification system and any others required.

AAMVA members are concerned that the NPRM suggests that states must include points on driver's licenses in the driver history of any database constructed as point systems and application of points vary from state to state. Members are also concerned about the prescriptive requirements that the NPRM notes should be maintained in a "motor vehicle database." AAMVA members are also troubled that states must provide all states electronic access to information contained in the motor vehicle database of the state in a **manner approved by DHS pursuant to this regulation.** AAMVA and its members must be involved in any system decisions and member states must have control over the information that is stored in their databases, who has access to that information and how it is used. This is another example of lack of clarity and concern in this NPRM, and AAMVA and its members are willing to continue to work with DHS to better understand the importance of defining the objectives and parameters of this verification system and

its interoperability. AAMVA members have considerable experience in this type of verification system as association members partnered with US DOT from conception to develop and implement the CDLIS.

AAMVA members would expect DHS to fund a system that advances interoperability, including costs for AAMVAnet, state-side system changes and connectivity. Again, AAMVA recommends that CDLIS system infrastructure and platform be used as the model to design, build and implement an all-driver system. AAMVA members remain interested in working with DHS to determine requirements, and to design and implement this system in a timeframe that is reasonable and meets the states' needs. AAMVA members are willing to work with DHS to consider alternate solutions to achieve this REAL ID Act requirement. AAMVA members have appreciated the discussion with DHS representatives and US DOT representatives on basic concepts of an all-driver system. Much more discussion is needed to help meet the basic requirements of the Act and to evaluate the costs and benefits of this type of system development, including risk mitigation and fraud reduction. AAMVA members believe that it is imperative for DHS to recognize that DMVs cannot use a stand alone system to achieve this requirement and that any type of verification must be integrated into the business processes and the existing systems used by the states, including AAMVAnet and CDLIS.

AAMVA members recognize that DHS is very interested in the governance of the verification systems and interoperability of systems to achieve the requirements of the REAL ID Act. AAMVA members are very interested in helping to determine the governance structure of any systems that potentially could interface with state driver licensing systems and federal verification systems. AAMVA members recognize the importance of system access, use and control. They also recognize the importance of security, and protecting the privacy of personal information. In order to ensure that careful consideration is given to all the components of governance and exactly what systems will be governed, AAMVA members are currently working on a proposal for DHS. It is not yet completed. On behalf of its members, AAMVA will file supplemental comments to this NPRM with governance recommendations. Those supplemental comments will also include a recommended prioritization of the required verification systems and document verification systems options based on risk and value. AAMVA members want to emphasize that governance of DMV related systems and any accompanying verification systems are critical to the states. While the structure for governance has yet to be recommended to DHS, it is imperative to note that states expect to have control over their systems, their information and the processes that govern any use or access. AAMVA members will remain acutely interested and active in a continued dialogue regarding system governance, system prioritization and data privacy.

## **DATA RETENTION AND STORAGE**

### **§ 37.31 Source document retention**

Document authentication and review are critical parts of the DMV credentialing process. It has been standard operating procedure in some states to retain copies of all documents used for issuance and renewal. States have documents, dating back years, stored in what are now varying formats and disparate systems. It is becoming a growing practice in most states to retain copies of source documents in an electronic format. States are moving to scanning, storage and retrieval technologies that minimize storage burden and make

archived documents immediately obtainable at distributed locations. This direction should address the underlying congressional intent in the REAL ID Act to assist law enforcement in investigations.

AAMVA members recognize the need to provide source documents to law enforcement for investigation and in general support the need for document retrieval and retention. Our members recognize this process as a best practice in the issuance of driver's licenses and identification cards. It should be clear that the images that are stored are basically black and white "electronic" copies of paper documents. The states that use document imaging, for the most part, only store in black and white; limit what is scanned and stored due to costly storage; do not link scanned documents with the driver record; and only allow limited access to the information, as it is considered highly personal and confidential.

The greatest issues of concern to our members in the data retention and storage area are those that deal with transferring document images and linking document images to the driver record. Many states do not have the most up-to-date data processing systems, nor do they have replacement plans on the books in the near future. Integrating document image storage with the driver record would be very costly. As well, transferring these images among states could be extremely costly. No infrastructure currently exists to handle document transfer among states. Requirements for any process of this magnitude cannot be determined in regulations, especially since technology changes so rapidly. States need to determine together what, if any, data transfer processes work best for them and their customers.

AAMVA members' recommendations for data retention and storage are:

- states should not be required to capture and store documents presented by an applicant to verify address of principal residence;
- states, working together, should be able to determine what documents can and should be transferred between states and to determine the technical requirements;
- color images should not be required, and
- while a state may opt for the operational efficiencies associated with integrating the image storage with the driver file, it should not be required as long as the image is retrievable.

AAMVA members request that DHS more fully consider the intent and necessity of some of the provisions in this section of the NPRM. For example, is it really necessary to keep an imaged copy of a social security card if the state completed electronic verification and the record is marked? As well, is it really necessary to keep the documents used to verify address? Central mail issuance should be sufficient to verify address. Image storage is costly, especially in high volume states. It can be unduly burdensome and time consuming without corresponding value or risk mitigation. States need flexibility in the data retention and storage area to determine what works best for their processes, systems and laws.

DHS needs to clarify its definition of source documents to outline exactly what it believes should be retained; that it is their intent to have different retention periods for electronic and paper copies; that an eight year renewal cycle coincides with a seven year document retention period; and that data retention and storage in this section of the NPRM applies only to documents, not photos. The requirement to color scan

and exchange documents using AAMVA's Digital Image Exchange program is misplaced. This effort only deals with photos and it would be a giant leap to consider its use for documents.

DHS should recognize that AAMVA members are required to abide by state document retention and purge policies and may need statute changes to implement this section of the NPRM. DHS should also recognize that source documents converted and stored as digital images, or retained in hard copy, may constitute public records and become subject to public record requests.

## **FRAUD PREVENTION AND SECURITY STANDARDS**

### **§ 37.15 Physical security features for the driver's license or identification card**

AAMVA members recognize that one of the most important components of any personal identification system is the finished card issued to the customer. The card serves as the most visible indication that the person is actually the individual described on the card and the holder has the privileges as described on the card. Driver's licenses and identification cards must be readily recognizable as genuine and must be fraud and counterfeit resistant.

AAMVA members have spent considerable time and effort on the development and design of a driver license and identification card specification that meets the needs of the motor vehicle and law enforcement community and that can evolve and change with technology and new threats.

The AAMVA *Driver Licensing/Identification Card Design Specification* was developed as one part of AAMVA's *Driver's License/Identification Card Security Framework* to improve the security of the driver's license and identification card. This Specification is the product of the involvement of a wide range of stakeholders, including government and non-government representatives such as law enforcement and forensic experts, industry experts in the area of card production and security, physical security experts, and users of the driver's license and identification card. As with all AAMVA programs, specifications and products, jurisdictional input drives the development and the Board of Directors approves the end product. This was the case with the specification.

The goals and intended results of the AAMVA *Driver Licensing/Identification Card Design Specification* are functionality, interoperability, compatibility, commonality and security. This Specification is the industry standard today and it provides the flexibility for change as conditions, threats or technologies dictate. States also can incorporate more than the minimum standards provided by the Specification. As card production contracts expire, and new bids are released, states are using the AAMVA *Driver Licensing/Identification Card Design Specification* as the minimum standard. Many states have already adopted its use. To change direction now would be costly for states.

As the Specification provides, states have increasingly recognized the need and benefit of including a range of physical security features and specifications in their driver's licenses and identification cards. Through AAMVA, they have codified a list of best practice features, which can be used in varying combinations to

achieve required security and optimum utility for the issuing agencies and law enforcement personnel who rely on them.

AAMVA standards reflect the collective research, best practice and standard industry practice, and they allow for effective competitive procurements.

As noted earlier, data stored on a driver's license machine-readable barcode and the magnetic stripe is typically unencrypted to ensure its availability to law enforcement personnel, courts and other jurisdictions. Capture of this information initiates the adjudication process for traffic violations. Encrypting such information, which is identical to that already printed on the front of the card, negates the advantages of automated data capture technologies to DMVs, law enforcement agencies and the courts. And, the management of a national, multi-jurisdictional "encryption key" system is unwieldy and it carries far reaching, expensive and potentially negative impacts on law enforcement communities.

States should be able to use the *AAMVA Driver Licensing/Identification Card Design Specification* as the standard for P.L. 109-13.

The card design specification in the NPRM recognizes the importance of document security features, the need for a well-balanced set of features with multiple levels of security and the need for integrated security features. But, the NPRM does not recognize the impracticality or the need for a "gold standard" in card design. The implied value simply does not correspond to the very real cost.

While many of the NPRM minimum card security features are in use today in both US and Canadian jurisdictions, AAMVA is not aware of any jurisdiction that uses all the noted security features with the proposed card stock in its card design or production. The application of variable data via laser engraving to ensure data is engraved into the layers of the card essentially dictates moving all over-the-counter issuance states to transition to central issuance. This feature cannot be applied with printers deployed in over-the-counter environments. And while the substrate material is not called out, the NPRM design specification essentially calls for polycarbonate material. This material is not used anywhere in the US today, is the highest cost card material in production today and is only available from a limited number of vendors. AAMVA members do not support the polycarbonate options as the only option for card material.

States should be able to determine their own driver's licensing and identification card issuance systems and not be constrained to one selected by a de facto central issuance card design specification as promulgated in this NPRM.

One state projects that adoption of the NPRM minimum recommended card design security features (the de facto polycarbonate and laser engraving requirement) will increase its cost to produce a license by 700 percent. AAMVA members recognize the need of continuing to provide counterfeit resistant technology to driver's licenses and identification cards. However, members and independent card security experts, also recognize there is no counterfeit-proof product. AAMVA's members contend that the card design security features in this NPRM are "a solution in search of a problem." The major fraud and abuse issues in DMVs have not been associated with the card; they have been associated with breeder documents that cannot be

verified, systems breakdowns and people who breach integrity. A driver's license or identification card can be altered, but security features are in place so the alteration can be recognized.

AAMVA members have consistently recommended that the REAL ID regulations include a statement of the performance requirements that the security configuration of a REAL ID compliant driver's license or identification card must meet, rather than specifying a particular set of security features to be used. DHS has recognized the need for performance requirements and the need for adversarial testing. The provisions surrounding both of these concepts in the NPRM are vague and need clarification. While there are card durability/security performance standards in use today in the states, DHS must recognize that there are no adversarial testing standards or criteria available nationally or internationally in the standards community. Establishing an adversarial testing program would require the development of a set of testing standards and procedures and the designation of independent testing organizations to carry out the testing. The federal government has resources, such as the National Institute of Standards and Technology (NIST). NIST might be able to assist DHS with the development of an adversarial testing program. We recommend that DHS take the lead to initiate development of a document security adversarial testing program and, when such a program is developed, that DHS take responsibility for the testing, using credentials provided by the states. AAMVA members need to be involved in any effort surrounding the development of performance or adversarial testing.

AAMVA members have also recommended that DHS initiate the formation of a document security advisory group composed of document security experts from the federal government to assist in the development of card security performance standards.

This area of the NPRM is of particular concern to members as it can have fundamental and fiscal impacts on the states, such as changing driver's license and identification card delivery systems, contract provisions, procurement decisions, and licensing costs. States cannot consider making any changes until existing contracts with card integrators expire or they will face high penalties for breaking existing contracts. Any change too would require states to proceed through the competitive bidding process, evaluate proposals, award new contracts, and implement the complex and expensive process of re-engineering their issuance processes. Any wholesale change in card design will be costly, complex and time consuming.

AAMVA members also point out that a specific technology will also reduce the ability of states to choose between competing security technologies and make cost effective purchases. Restricting all state-issued driver's licenses and identification cards to a single security configuration could introduce new security vulnerabilities rather than protect the driver's license and identification card against fraud. If all driver's licenses and identification cards have the same basic configuration, counterfeiters will only need to overcome one configuration to be able to counterfeit any jurisdiction's card. This is a significant security concern.

AAMVA members ask that DHS clarify the requirement for independent testing, the approach being contemplated for card performance and its reasoning behind the proposed card design security features.

### **§ 37.41 Comprehensive security plan**

States recognize the need for physical security of their issuance facilities and of vendor production facilities. They also recognize the importance of inventory control, securing equipment and ensuring that the inventory chain is secure throughout the distribution channels. A state's security challenges are multiplied in over-the-counter, decentralized facilities and many of AAMVA's members operate over-the-counter driver's license and identification card issuance systems. The NPRM's proposed card specifications and the physical security requirements required in § 37.43 may very well force all states to a centralized card issuance process. It also is a move that could be costly and certainly cannot be accomplished without an extensive transition period.

The concept of a security plan for DMVs is not new as administrators routinely face issues that potentially threaten public and employee safety and, in isolated cases, have had to respond to breaches in security. AAMVA members support the concept of a security plan but are concerned that the plan and the NPRM recommended security requirements create standards which exceed those reasonably necessary.

The NPRM requires states to prepare a "comprehensive security plan for all state DMV offices and driver's license and identification card storage and production facilities." Security requirements should be more clearly defined for a production facility and DMV field offices. The development of this plan and the 11 items enumerated will be a major and costly undertaking for states, especially those with decentralized facilities. Some states have well over 100 issuance locations. Item (11) asking for other information as determined by DHS is far too broad for states to determine the extent and effort of their security plans.

AAMVA members recommend that DHS clarify what constitutes the required "written risk assessment of each facility." A clarification and a template would be useful for the states. AAMVA members remain interested in working with DHS to develop reasonable facility security expectations that can meet the intent of the Act and do so from a risk/value perspective.

In the fraudulent document training area, AAMVA seeks clarification on the meaning of "domain awareness" training. AAMVA members support fraudulent document recognition training. As part of its *Driver's License and Identification Card Security Framework*, AAMVA has developed a comprehensive Fraudulent Document Recognition Training program that has been deployed in many jurisdictions. As states are familiar with this program and have rated it favorably, AAMVA members recommend that it be noted in the NPRM as a DHS approved training curriculum to meet the Act's requirements. AAMVA jurisdictional members designed the training curriculum.

Another area that needs clarification under this section is the requirement that the security plan address confiscation of driver's licenses or identification cards fraudulently issued in another state. The confiscation requirement has the potential to place DMV customer service employees in harms way by requiring them to seize original credentials from applicants who may not want to give them up. Physical confrontations are bound to develop and many states do not staff their offices with law enforcement or other personnel capable of physical intervention. The practical implications of attempting to locate and confiscate the credential after the applicant leaves the facility are also flawed. It is unlikely that someone attempting to

pass off fraudulent source documents at a DMV office will provide enough valid information to assist in locating them after they leave. For these reasons, we believe the individual states are in a better position to determine if confiscation of credentials should become a requirement.

As states move toward compliance and submit their security plans, AAMVA members request that DHS afford these plans the same level of confidentiality that will be given to the states' certification plans. These plans cannot be subject to public information requests.

### **§ 37.43 Physical security of DMV facilities**

In both centralized and decentralized issuance systems, DMVs have put in place sophisticated security systems including hidden cameras, audible and silent alarm systems, access control systems and other measures that are not routinely shared. States have also incorporated physical and logical security into their contracts with their license issuance vendors. This information is not shared publicly. States will share the information as part of their annual certification.

AAMVA members recommend that DHS not use the NASPO standard to specify the security of driver's license or identification card manufacturing operations. Instead, AAMVA and its members would like to work directly with the Department to develop a set of best practices in this area. This standard is inconsistent with the type of business conducted at a very open, public driver license issuance office. The standard was established for a manufacturing facility. DMV offices are not manufacturing facilities with controlled access. Customers use these facilities. This type of standard will most likely force states to a central issuance system. DHS should explore solutions that will provide security in an over-the-counter environment and a central issuance environment. AAMVA members recommend that DHS commission a working group of state DMV administrators to develop an appropriate set of standards and best practices specifically for DMVs that have both central and over-the-counter issuance methods. Until a reasonable standard is developed, states should continue to have the flexibility to determine what works for their issuance and production networks.

Plainly, NASPO is an inappropriate physical security standard for the DMVs.

AAMVA members seek clarification from DHS if facilities that issue interim driver's licenses and identification cards provided to customers until their permanent credentials are mailed from a central facility are subject to the physical security standards in the NPRM.

AAMVA members recommend that AAMVA's current system, the Fraud Electronic Warning System (FEWS) be used to disseminate information regarding potential or suspected fraud that occurs at DMVs. This system is used by DMVs and law enforcement across the US and Canada and has been successful in identifying, combating and communicating fraud issues. Its use has been tested and its value recognized by law enforcement officials and DMV administrators.

**§ 37.45 Background checks for covered employees.**

The NPRM does recognize that states should have the flexibility to determine which employees undergo background checks and it is assumed that DHS will allow states ample latitude to continue to make these determinations. However, the extent and the requirements of background checks are concerning.

Most states currently only undertake background investigations at the time of hiring, and of the 29 states that currently carry out some level of employee background checks, only two conduct credit checks. The requirement to complete FBI finger print checks is costly, averaging around \$24 per person. There is also in some cases a state cost to complete these investigations. The requirement to ensure that all designated employees, including those who are already employed, undergo background investigations will have a significant impact on many states' labor contracts and personnel practices. Numerous employees were hired under terms and conditions not requiring a security clearance. Should these employees be disqualified under the new regulations, states may be obligated to provide them with alternative employment or severance.

States could also face additional costs associated with recruiting, hiring and training replacement employees. It is recommended that the flexibility provided in the NPRM be further expanded to provide states maximum flexibility to implement the regulations in a manner that is specific to the needs of their state and that avoids unnecessary confusion and disruption in services.

Specifically, all existing employees should be "grandfathered in", and states can determine if they want to complete background investigations on these employees or not. States should determine what, and in what manner, new employees should receive background checks. Financial checks should not be a requirement because of their cost and states' governing personnel rules. Lawful presence checks are a redundancy and an excessive and unnecessary requirement since most states have systems in place to ensure that government employees are US citizens or lawfully present. It is not possible to put employees who were hired for a specific classification into another classification until a background investigation is completed. New hires should be granted provisional clearance pending results of any background check to ensure a state's ability to compete and hire needed staff.

All of these issues are a bargaining issue with the respective unions in the states.

**COMPLIANCE**

**§ 37.05 Deadlines and validity periods for REAL ID driver's licenses and identification cards**

It is appreciated that DHS recognizes that a May 11, 2008, implementation date is difficult for states to meet and that there is a need for a date-forward re-enrollment period. The May 11, 2013, suggested compliance date for completed re-enrollment is still not enough time.

In its survey of states underpinning the AAMVA-NGA-NCSL REAL ID Act National Impact Analysis issued in September 2006, AAMVA assumed a five-year re-enrollment period. A five-year re-enrollment

period places an onerous operational and fiscal burden on the states -- nearly \$8.5 billion. DHS has, in the NPRM, effectively compressed that timeframe to three years. Costs are sure to exceed \$8.5 billion.

AAMVA assumes that any of its members who intend to implement P.L. 109-13 will request an implementation extension to January 1, 2010. This extension is not only practical but required because of DHS' lack of publication of regulations in a timely manner. Based on DHS lack of time sensitivity to providing lead time to the states for implementation, it is unrealistic for the Department to propose a compressed timetable for re-enrollment based on states' need for an implementation extension. The NPRM's re-enrollment deadline of May 11, 2013 is wholly infeasible and unrealistic for any state-large or small. Giving states three years to re-enroll almost all of their drivers and identification card holders is literally an impossible task.

AAMVA members continue to recommend a 10-year re-enrollment period from the implementation of the Act by the states. Further, AAMVA members recommend that:

- in addition to exempting those persons born before 1935 from re-enrollment, this exemption be broadened to allow for a waiver of verification requirements to facilitate applicants who have already been through an identity vetting process by the federal government (e.g., military ID, federal employee credential),
- allow applicants with valid and compliant REAL ID document(s) to transfer from state-to-state without further documentation other than proof of residence and lawful presence,
- exempt segments of applicants based on certain requirements related to applicable risk such as year of birth or duration of continuous relationship with the state of licensure, and
- allow states to determine other exemptions based on their own processes and systems.

For example, states should have the opportunity to "grandfather in" current driver's license and identification card holders if critical information such as social security number and photo image matching has been completed. States have already done considerable data cleansing of those systems, and they know the issues of unmatched information and duplicate photos and records. Approaching re-enrollment as an exceptions process versus a blanket re-enrollment would significantly reduce the costs and operational issues associated with the proposed NPRM re-enrollment recommendations.

It is possible that the entire driver's license and identification card issuance system could experience a "melt down" if the NPRM approach to re-enrollment is implemented. The increased workload attributed to re-enrollment over a three year period will far exceed the existing capacity of most state licensing agencies. A majority of states indicate they are operating at full capacity to meet existing demand. If states are to maintain their present levels of service, while incorporating the added transaction volumes mandated by P.L. 109-13, states will need to: hire additional employees and increase service hours; expand or increase the number of facilities to accommodate additional customer volume; purchase additional equipment to support personnel; create and implement public education campaigns to inform customers; and anticipate and handle increases in calls, complaints, and return visits due to confusion and adjustments resulting from the new requirements.

Re-enrollment alone will require significant investments in DMV systems, personnel and facilities. However, even if full funding were provided, meeting the three-year re-enrollment deadline would result in severe customer service disruptions due to the increase in annual transactions.

Providing states with flexibility to manage re-enrollment and to do so over a greater length of time would still meet the objectives of the Act while reducing the fiscal impact on states and minimizing service disruptions for customers. Clearly, no additional verification can be required beyond what states currently do absent real time, efficient, reliable, verification systems contemplated in this NPRM.

While the majority of states have current driver's license and identification card durations equal to or shorter than eight years, durations as long as 10 years do exist (at least one state allows a duration to age 65.) Conformity with this provision will require state legislative change, and result in increased costs and service demands for those jurisdictions being required to shorten their license periods.

### **§ 37.51 Compliance—general requirements**

State DMVs are accustomed to federal oversight and certification procedures. They comply now with certifications required by the US DOT including the Federal Highway Administration (FHWA), the National Highway Traffic Safety Administration (NHTSA) and FMCSA. The keys to these audits and certifications are that states have ample preparation time, the process is streamlined and usually the federal agencies conduct on-site visits for short periods of time. In most cases, they are not overly burdensome as they are conducted periodically at established and expected times. AAMVA members are concerned that the DHS certification procedures for initial certification and annual certifications are too burdensome on states because they will require huge administrative efforts and administrative costs. Some states may not have the personnel to complete the required certifications and may have to hire contractors. A DHS certification schedule that conflicts or overlaps with a FMCSA Commercial Driver License Program audit could be doubly concerning.

### **§ 37.55 Initial state certification**

It is important for DHS to recognize that not all DMVs are under a governor's jurisdiction. Some DMVs are under the auspices of an elected secretary of state, an attorney general or a mayor. The rule should provide that the certification be signed by the highest-ranking state official overseeing the DMV including the DMV Administrator.

It is recognized that the NPRM requires a letter from the attorney general of the state confirming that the state has the statutory authority to meet the standards including all the regulations, administrative procedures and practices. DHS too should recognize that the statutory and regulation development process in states takes an inordinate amount of time. That process at the state level is dependent on final regulations from DHS. One state notes that, assuming final regulations are published as early as August 2007, it will not have their final state regulations until October 2008. Considering advance testing time that leaves less than a year to be ready for implementation by December 31, 2009.

### **§ 37.57 Annual state certifications**

AAMVA members recommend that states work with DHS in the development of a streamlined self-certification process to meet the requirements of the Act. This would include coordination with other existing audits and audit entities having considerable content overlap such as US DOT's FMCSA.

AAMVA members also recommend that states choosing to participate in the *Drivers License Agreement* may substitute its compliance review process in lieu of DHS audit requirements.

### **§ 37.67 Non-REAL ID driver's licenses and identification cards**

DHS regulations and standards should not govern the issuance of non-REAL ID credentials. As noted previously, the "branding" of the credential is misplaced. The focus should be on "branding" REAL IDs. States should only have to mark REAL ID compliant credentials, not mark non-REAL ID compliant credentials. A standardized design or color should not be used for non-REAL ID compliant credentials. Many states may not comply with P.L. 109-13 and believe they should not have to comply with this requirement on the face of the card or in the machine readable zone. A standardized color or design is also not supported by AAMVA members. Any "uniqueness" can lead to complacency that would detract from a careful inspection of the credential.

As noted, the AAMVA *Driver Licensing and Identification Card Design Specification* is recommended for driver's license and identification cards. While it includes standard and minimum features, it also allows for features that retain state identity and control over the general look of the driver's license and identification card.

## **EXTENSION**

### **§ 37.63 Extension of deadline**

After a 22-month delay, to publish an NPRM that at the same time remains vague and calls for draconian measures, it is inconceivable that DHS would expect the states to be anywhere near ready to begin implementation of the massive mandate by December 31, 2009. Even if the verification systems were in place, states still need more time to secure state enabling legislation, re-bid contracts, develop and issue new contracts, make system modifications (including new builds), change processes, prepare customers and find funds absent any federal assistance. Effectively, a one and a half year window exists (August 2007 – March 2009 for testing) for states to be ready for implementation by December 31, 2009. That expectation is unreasonable and unrealistic.

The proposed extension further backs states against the wall with the extensive re-enrollment required by May 11, 2013. Only a three-year window to re-enroll all existing drivers and identification card holders is similarly unrealistic. More than one half of AAMVA's US members have four year or longer renewal cycles. Added to this burden would be the requirement for verification to serve in-person many customers who may have license or identification card changes (such as name or address) outside their normal renewal

cycle and to serve in-person any customer who may have had his or her license or identification card lost or stolen.

AAMVA members cannot overemphasize the extensive effort that would be required for states to meet even parts of this NPRM by December 31, 2009. While it is better than the May 11, 2008 Congressional deadline, it still is virtually impossible to meet.

There are also remaining concerns that the NPRM still lacks clarity. The earliest states will fully understand or realize what the final NPRM requires is July 2007. States must have another opportunity to review the input that has been received during the NPRM comment period and DHS' disposition of those comments.

Assuming there are federal funds available and states want to comply, there are a number of alternatives for a schedule that DHS should consider. With the expectation of a reasonable final rule, based on AAMVA member input, one option is to consider an extension to December 31, 2020 and allow states to phase in their implementation strategically over the next several years addressing those less intrusive parts of the statute that can be accomplished sooner (like the application process) and subsequently addressing more complex provisions, working at a pace that realistically conforms to their operating environment. This would assume that the federal government would also do its part in designing and implementing the verification systems, the card performance specifications and funding. This approach would allow states and DHS time to address the critical path items for compliance (that have no schedule now) in a reasonable, phased manner--especially the verification systems that are not yet designed, that need improvements or have that not yet been implemented. This approach would give DHS and Congress time to secure implementation and ongoing federal funding and it would give the federal government time to address the disparate naming conventions in their databases.

Another alternative is to extend the compliance deadline from December 31, 2009 to five years after final regulations are published for issuance and 10 years for re-enrollment. This alternative, as well, is predicated on a more reasonable final rule which accepts AAMVA member recommendations. This alternative would also give DHS and Congress time to fund this mandate, build the verification systems for state connection and address the disparate naming conventions in the federal databases.

As evidence of the time it takes DMVs to make major program, process and system modifications, the Motor Carrier Safety Improvement Act (MCSIA) was passed by Congress in 1999 and states were to be in compliance by September 30, 2005. Seven years after passage, many states are still not in full compliance and some just became compliant. While the MCSIA had considerable system interstate data transfer challenges through CDLIS, these challenges pale in comparison to REAL ID.

AAMVA members recognize the importance of improving the issuance system. States continue to use the *Driver's License/Identification Card Security Framework* as a guide. States also are cleaning up their databases to detect fraud and are implementing risk mitigation strategies regardless of REAL ID. These efforts should be recognized as compliance provisions.

AAMVA members would be happy to work with DHS on devising an implementation and re-enrollment schedule that meets the members' needs and assists those who plan to comply.

Finally, extension authority must be granted consistently for all states. When a legitimate reason for extension exists for one state, it should apply equally to all states. DHS must exercise flexibility in allowing states time to apply for an extension. If final regulations are not issued until, e.g., August 2007, an October 2007 request for an extension deadline leaves states with little time to fully consider the implications of compliance and/or to seek legislative approval.

### **SPECIFIC DHS REQUESTED RESPONSES FROM COMMENTERS**

AAMVA members appreciate that DHS is requesting comments on a number of areas of this NPRM and, where appropriate, will comment and provide input. It is, however, concerning that so many foundational aspects of this NPRM have yet to be fully fleshed out. AAMVA and many other organizations have provided valuable input since the Act was first introduced in May 2005. AAMVA's *Driver License/Identification Card Security Framework*, a benchmark for driver's license and identification card issuance and product and process improvements, was provided to DHS. In February 2006, AAMVA, NSCL and NGA provided state implementation considerations to DHS and in September 2006, AAMVA, NSCL and NGA provided the *REAL ID Act National Impact Analysis* with recommendations to DHS. AAMVA hosted a forum on card security features for DHS in Williamsburg, Virginia last year, and also submitted white papers on both card security and physical premises security to the agency. While AAMVA members appreciate the complexity of this NPRM and the REAL ID Act, it is clear that many uncertainties remain that have yet to be fully vetted.

With DHS requesting specific comments in so many key areas, AAMVA members again reiterate that it is necessary a second notice of proposed rule making be issued, along with extended deadlines, prior to advancing this NPRM to its final format. Too many issues remain to be fully vetted after this initial comment period to move this NPRM to a final rule.

**1. In addition to security benefits, what other ancillary benefits could REAL ID reasonably be expected to produce? For example, could REAL ID be expected to reduce instances of underage drinking through use of false/fraudulent identification? If so, please provide details about the expected benefit and how it would be achieved through REAL ID.**

States have clearly understood and promoted the safety and security benefits of securely issued driver's licenses and identification cards and have put in place many mechanisms to provide not only the intended benefit of a credential to drive but also to provide ancillary benefits. License designs and state processes such as image matching and social security number verification are already addressing highway safety concerns such as underage drinking and duplicate license issuance. The vast majority of fraudulent licenses and identification cards used in instances of underage drinking are overtly counterfeit when observed by even a casual observer. Bar and liquor store owners increasingly rely upon equipment that allows them to read the barcodes on licenses and identification cards to determine if the document is legitimate and to record the patron's age. AAMVA members have consistently supported the need to enhance the licensing

process and the basic safety tenet of one driver, one record through the *Driver License Agreement*. If effectively and realistically implemented, the concepts surrounding REAL ID could further improve the issuance process and the ancillary benefits of ensuring an individual's identity. The most important contributors to these ancillary benefits are real time data verification systems with strong data integrity that provide the states with cost effective use. The NPRM remains vague on how these systems will operate, their implementation costs to the states, and the required transaction costs. So, it remains unclear just how "real" the ancillary benefits will be with REAL ID versus the practices and improvements states are already making in identification security and issuance.

Some of the prescriptive rule provisions may have unintended consequences and be detrimental to highway safety and security. For example, if every address change requires an in-person visit to the DMV, it is likely that citizens will not comply with address change requirements which make conviction notification and processing much more difficult. This would be an ancillary detriment.

**2. DHS seeks comment on the proposed scope of "official purpose," and how DHS could expand this definition to other federal activities.**

AAMVA members are pleased that official purpose was limited to accessing federal facilities, boarding commercial aircraft and entering nuclear power plants. AAMVA members also are pleased that the regulations are not intended to change current admittance practices to federal facilities. AAMVA members remain concerned with the unilateral ability for the Secretary of DHS to expand this definition in the future without consultation and without any parameters such as a national security threat. The definition of "official purpose" should not be expanded beyond the narrow interpretation currently given by DHS. AAMVA members too are concerned with the impact this definition will have on drivers in states who choose not to comply with P.L. 109-13. DHS should advise on the process or alternate form of identification that will be accepted from drivers who need to access federal facilities such as military bases or nuclear power plants and may not have a REAL ID compliant credential.

**3. Whether the list of documents acceptable for establishing identity should be expanded. Commenters who believe the list should be expanded should include reasons for the expansion and how DMVs will be able to verify electronically with issuing agencies the authenticity and validity of these documents?**

AAMVA members have been strong proponents of limiting the identity documents required, and made similar recommendations to those noted in the NPRM in its *Driver's License/Identification Card Security Framework*. The *Framework* recommends that all U.S. jurisdictions use the "Acceptable Verifiable Resource List" for the United States. This is a limited list of documents that uses specific data elements found on the source documents to determine a customer's identity. No foreign documents other than a passport are recommended for non-US citizens. AAMVA members do not believe the acceptable documents list in the NPRM should be expanded, but it does strongly recommend that the federal government assist the states in issuing identity documents that have consistent naming conventions. Passport naming allowances are dissimilar to social security card naming allowances. It is difficult for a state DMV to determine full legal name with the identity documents presented if the federal government

does not address its own internal shortcomings in naming conventions. AAMVA members also recommend that DHS review the list of immigration documents recommended to establish identity. As well, it is critical to recognize that DMVs will need to employ exception processing on any list of documents as they deem circumstantially appropriate. AAMVA members also caution DHS that the final rule should be flexible enough to allow for additions, deletions and/or changes to an acceptable documents list. This flexibility is critical as DMV processes, systems, procedures and technology can change.

**4. Whether individuals born before 1935 who have established histories with a State should be wholly exempt from the birth certificate verification requirements of this regulation, or whether, as proposed, such cases should be handled under each State's exceptions process.**

These individuals should not only be exempted from the birth certificate requirements as specified in the NPRM, but they, and many other similar situational groups/individuals, should be wholly exempted from the entire re-enrollment process. If DHS' prime concern is security, it surely is not these individuals who pose any potential threat. The same logic applies to many other groups of established customers who have a history with the DMV and where DMVs have deployed data clean up processes to address potential fraud. The need to wholly exempt individuals from the entire re-enrollment process is outlined in AAMVA's response to this rule. Currently, states are very adept on deploying exception processes to address unique situations but these types of overarching common sense applications should not be pushed to an exception process at each transaction. It is incorrect to assume that only those citizens born before 1935 do not have birth certificates. States have indicated that many rural counties as well did not provide birth certificates to those born much later than 1935. The Department should focus on risk-based populations. If DHS is compelled to only consider a birth year as an exemption, consideration should be given to a formula such as exempting those citizens born before 1951 who have 10 or more years of consecutive history with the state DMV and have successfully passed a social security number verification (which would verify lawful presence) and any other verification the state deems appropriate. States still should be able to set their own re-enrollment parameters.

**5. How DHS can better integrate American Samoa and the Commonwealth of the Northern Marianas into the REAL ID framework.**

It is unclear what DHS is referring to with "integration" in this question. American Samoa is a member of AAMVA and AAMVA will be happy to work with the Commonwealth of the Northern Marianas to share information.

**6. Another classification of persons that would be unable to present a visa are Canadians who enter the United States without having to obtain a visa and who stay in the United States for extended periods (i.e., more than 90 days) at a time. While the majority of these are short-term visitors who would not need a U.S. driver's license, and indeed are not issued any U.S. documentation or recorded in U.S. nonimmigrant data systems, some are longer-term visitors who may be students, authorized workers or others who may have reason to need a U.S. license. DHS requests comments specifically on how this group could be affected if they are unable to obtain a U.S. REAL ID driver's license that could be used for Federal purposes.**

It is wrong to assume that these longer term Canadian visitors do not need a U.S. license for extended periods of time. AAMVA expects CCMTA will provide additional impact details. Many states have statutory language that defines when a person must obtain a driver's license that are usually tied to how long they are in the state, employment status, whether they have children enrolled in school, etc.

**7. Native American Tribal Documents. DHS discussed these documents with the Bureau of Indian Affairs of the Department of the Interior and concluded that since all tribes obtain State-issued documentation to verify birth; all tribal members will have, or can obtain, an eligible identification document, rather than using tribal documents. DHS solicits comments on whether these or any other documents should be included as acceptable documentation for showing identity. Commenters should address instances in which classifications of individuals could not obtain any of the documents already on the proposed list, issues of reliability of the document proposed, and ability of the States to verify the proposed document. If DHS concludes that other documents, including those listed above and others submitted by commenters are reliable and can be verified electronically by the States, they may be included as acceptable identity documents in the final REAL ID rule.**

AAMVA members recommend that the documents listed be used as the base documents for all US citizens. DMVs have exception processes in place to deal with unique circumstances and expect to continue to use those exception processes where warranted with REAL ID.

**8. The EAD is envisioned as the document to be presented by the following classes of REAL ID-authorized aliens: Temporary Protected Status (TPS) aliens; asylees and asylum applicants; refugees; adjustment applicants; and aliens granted deferred action. DHS understands that regulatory limitations on issuance of EADs to asylum and TPS applicants will result in a wait period before these aliens will have acceptable documentation, and invites comment on what alternative documentation regimen may serve for these groups, and whether those groups need a REAL ID driver's license or identification card before their applicable wait period expires. The proposed rule also does not include immigration documentation showing any status under the immigration laws of American Samoa or the Commonwealth of the Northern Marianas for aliens within those jurisdictions. REAL ID specifies U.S. immigration statuses. DHS invites further comment about how these jurisdictions may better be integrated into the REAL ID framework.**

It is incorrect to assume that states will issue two types of driver's licenses and identification cards, REAL ID compliant and non-REAL ID compliant. While these driver's licenses and identification cards may be "temporary," they still would be REAL ID compliant in a state that chooses to only issue REAL ID compliant driver's licenses and identification cards. AAMVA members believe that expanding federal immigration documents and providing "alternative" or "interim" documents to those noted aliens above would only further complicate an already complicated federal immigration document system that taxes DMV front line employees and confuses customers. AAMVA's members' position is that any immigration document or status should be verifiable in SAVE in a real time, cost effective manner so that the documents are secondary and the electronic verification is primary. The SAVE system does not have these capabilities now but must be a fully functioning, real time, up-to-date system for states to adequately verify immigration documents. Past state history has revealed that some immigration and customs agents cannot be certain of

the face validity of some types of immigration documents. Electronic verification is necessary with a system that works properly and cost effectively. The bottom line is, DMV employees on the front line should not have to be immigration inspectors. The decision on whether a customer has lawful status in this country must come from the SAVE system and it must be absolute

**9. How DHS can tailor the address of principal residence requirement to provide for the security of classes of individuals such as federal judges and law enforcement officers.**

States understand the need for confidentiality and the risk associated with any access and/or release of the identity or address of any officer of the court or law enforcement officer. They do this now for a wide range of entities. Many of these transactions are handled "off system" and in a manner that states do not and cannot discuss openly. Therefore, they will not be outlined here. AAMVA members recommend that DHS permit the states to continue to handle this as they do now -- silently and confidentially.

**10. Whether the data elements currently proposed for inclusion in the machine readable zone of the driver's license or identification card should be reduced or expanded; whether the data in the machine-readable portion of the card should be encrypted for privacy reasons to protect the data from being harvested by third parties, and whether encryption would have any effect on law enforcement's ability to quickly read the data and identify the individual interdicted. What would it cost to build and manage the necessary information technology infrastructure for State and Federal law enforcement agencies to be able to access the information on the machine readable zone if the data were encrypted?**

Data elements should follow the AAMVA *Driver Licensing and Identification Card Design Specification* and the mandatory elements noted for the Machine Readable Technology (MRT). DHS has this specification. As noted earlier, capturing all changes and especially name changes is not supported by AAMVA members. Encryption of information contained in the MRZ of the card should not be required, especially due to its potential impact on law enforcement but also other authorized users of the credential and the current ability to use the MRT to detect fraudulent licenses and identification cards. P.L. 109-13 would indeed be a detriment to deterring underage drinking if bars could not easily use the MRT. It is impossible to predict the cost to build, manage and operate an encryption (key) infrastructure.

**11. DHS seeks comments on how best to secure the data, or whether or not to employ protections for the data encoded on the 2D bar code needs to be protected at all, while permitting law enforcement access and what technologies may be available to accomplish this balance. DHS is interested in comments that address whether a technology, such as the National Law Enforcement Telecommunications System (NLETS), or other system currently being used by law enforcement, could be used by the States to provide law enforcement ready access while maintaining the security of the information on the driver's license or identification card.**

These types of measures, while viewed by some outside the law enforcement and motor vehicle communities as protecting privacy and security, do very little to do so. The same information in the 2D bar code is the same information on the front of the license. Efforts here are misplaced and should be redirected

to strengthening laws for use of the data. Swiping the data on a license at a bar to verify age is an intended and legitimate use. Using that data for subsequent marketing purposes is an unintended use that should be better controlled through the passage and strict enforcement of laws at both the state and federal level.

**12. DHS requests comments on what data elements should be included in the machine readable zone and the privacy considerations regarding the selection of such data elements and this technology.**

AAMVA members recommend that DHS use the *AAMVA Driver Licensing and Identification Card Design Specification*. This is the standard states have put in place and are moving toward as contracts are re-bid or renewed. There is no need to reinvent the wheel.

**13. DHS seeks comments on whether a demonstrable law enforcement need exists to include address in the MRZ portion of the REAL ID driver's license, as currently proposed in this rule.**

Law enforcement uses all the information in the MRZ to reduce their administrative burden at roadside and to ensure that a license has not been altered. Address is a critical component of this information. It is used and is critical to the technology used at roadside by law enforcement at both the state and local levels.

**14. If a State chooses to produce driver's licenses and identification cards that are WHTI-compliant, whether citizenship could be denoted either on the face or machine-readable portion of the driver's license or identification card, and more generally on the procedures and business processes a State DMV could adopt in order to issue a REAL ID driver's license or identification card that also included citizenship information for WHTI compliance. DHS also invites comments on how States would or could incorporate a separate WHTI-compliant technology, such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF417 barcode requirement.**

AAMVA members are glad to see that DHS recognizes the need for some states to use the REAL ID in response to WHTI compliance and that the agency is moving forward with a pilot project in Washington State and British Columbia. This is an important direction for states that border Canada in helping to ensure the free flow of commerce and travel between the US and Canada.

**15. A State must take reasonable measures to ensure that the individual seeking the renewal is the same person to whom the REAL ID driver's license or identification card was issued. DHS is considering how best to authenticate the identity of an individual requesting renewal of his or her driver's license or identification card remotely, to guarantee that the REAL ID driver's license or identification card is being reissued to its proper holder. For example, DHS proposes that the State may choose to authenticate the identity of a renewal applicant through use of personal identifiers such as PIN numbers or questions whose answers only the proper holder would know, or through use of biometric information. DHS requests comments on these renewal procedures, including suggestions on any alternative approaches for remote renewals and authentication of remote renewals.**

AAMVA members are willing to assist DHS in any way to facilitate the states' abilities to continue their renewal functions in an efficient and cost effective manner with minimal impact on the customer. Some states have used PINs to authenticate driver's license and identification card renewals. The use of a PIN is a possibility; however, there should be a more sophisticated model that could be considered with input from private industry and technology vendors who are familiar with DMVs. Perhaps a method similar to credit card verification could be considered but the infrastructure and administration requirements would need to be carefully considered. This type of requirement cannot be determined without detailed discussions with DMV experts.

**16. This section of the NPRM will summarize the requirements of the Act that potentially have the greatest impact on privacy, the extent to which those requirements change current State driver's licensing practices, and how DHS intends to address privacy concerns regarding the Act. This analysis will address the three key privacy issues posed by the Act: (1) the connectivity of the databases; (2) the protection of the personal information stored in the State databases; and (3) the protection of the personal information stored on machine readable technology on the DL/IDs. DHS invite comments on whether the steps outlined below and otherwise discussed within the NPRM are appropriate and adequate.**

AAMVA members have outlined the importance DMVs place on privacy in this response to the NPRM. DMVs are very much aware of the need to keep driver information protected and confidential. AAMVA will address privacy in a supplemental filing.

**17. DHS requests comments on recommended best practices for protecting the privacy of the personal information stored in the various State motor vehicle databases pertaining to the requirements under this Act.**

States use information technology standards and tools such as encryption, intrusion detection and fire walls to ensure that information contained in their central databases is secure. Many of these standards do not solely relate to the DMV but are deployed at the state enterprise level. Such tools as information security audits, individual employee access audits, employee confidentiality policies and privacy and security plans are used in many DMVs. As antiquated systems are replaced, states are moving to business intelligence tools and advanced system security tools to ensure that information is only used for intended purposes and that layers of security are in place at many levels. DHS may also want to consider International Organization for Standardization (ISO) standards for information security management.

**18. How the Federal government can better assist States in verifying information against Federal databases.**

The federal government can best assist the states in assuring that naming conventions are consistent and/or algorithms are robust enough to ensure that matches can be made with as little manual intervention as possible. It can fund the development of these systems, especially the all-driver system required to verify driver's licenses and identification card issuance among the states. It too should fund the required state-end and AAMVAnet connections and ensure that states do not have to pay transaction fees to verify any information as required for this federal mandate. AAMVA members have extensive experience in using the

SSOLV and SAVE systems. DHS and the Social Security Administration have been advised of the current issues and the required upgrades necessary to improve reliability, functionality and data integrity issues. AAMVA has engaged task groups of expert members in business and systems to look at all the required verification systems. A recent discussion on verification systems between AAMVA members and DHS was very productive and it allowed DMVs to further outline for DHS the complexities of driver's licensing and identification card issuance systems. DHS should continue to engage AAMVA members in any discussions regarding verification of information, systems used to provide verification information and governance of these systems

**19. How the REAL ID Act can be leveraged to promote the concept of “one driver, one record, one record of jurisdiction” and prevent the issuance of multiple driver's licenses.**

AAMVA members have historically been supportive of the one driver, one record concept and have supported the *Driver License Agreement* compact and the adoption of this agreement in the jurisdictions. The key to ensuring that individuals only have one license is based on the same concept that the Commercial Driver License Information System (CDLIS) is based upon – a nationwide pointer system with the driver record and driver history transferred to a ‘change state of record’ when the driver moves to a new state. The same concept can be applied effectively with an all-driver system. While ideal and recognized as important for highway safety by NHTSA, the funding for such a system has not yet been provided. AAMVA and NHTSA's digital image exchange project will also assist in identifying multiple state license holders. Both of these projects can be accomplished with or without the REAL ID Act and would have positive impacts on fraud reduction and highway safety. Some states currently complete prior state of record checks when issuing new licenses to ensure that the license is valid as well as checking the NDR's PDPS. The recognition by DHS of the value of these programs with respect to REAL ID and identification of funding sources to implement and maintain them will enhance states abilities to adopt and develop them.

**20. DHS seeks comments on whether the proposed adversarial testing standards will lead to the development of a secure document solution that deters amateurs from producing deceptive counterfeits and/or alterations. DHS also seeks comments on other alternative approaches DHS could pursue on document security to achieve the same objective and how those approaches compare to a performance-based independent adversarial testing. DHS requests that States specifically comment on what contractual issues, if any, the States will face in satisfying the proposed document security requirements if the State's existing license fails one or more of the proposed adversarial tests.**

As DHS has not clearly outlined or defined the expected performance standards to test against, it is difficult for AAMVA members to comment on this question. DHS needs to clarify and quantitatively define the performance standards and associated adversarial testing requirements as well as the potential testing labs that would qualify to provide state certification. AAMVA members support and have recommended performance-based card security standards and adversarial testing. DHS is cautioned that the development of these standards will take time. AAMVA members have recommended that the AAMVA *Driver Licensing and Identification Card Design Specification* be used as the required standard for card security. States cannot consider meeting new standards until contracts are up for re-bid or renewal. With clear testing

criteria and performance standards, agreed to by the states and with input from vendors, states would be in a better position to meet the standard.

An option for adversarial testing would be for DHS to take responsibility for the process. States will already be overburdened by implementing other elements of the REAL ID Act. It would be very time consuming, expensive, and of limited value because states will be using card printing and assembly techniques developed by established vendors who sell security as the cornerstone of their product. Rather than have 56 jurisdictions contracting for their own testing, this is a process that could better be performed by DHS using documents supplied by the states. Having one agency responsible for coordinating the analysis would mean a higher level of confidence in the results and a more disciplined approach to the analysis protocols. Further, it is logical to assume that if a state has complied with the physical security requirements of the rule and one or more of its products do not pass the analysis, the same failures will probably occur in other jurisdictions. A centralized testing program would be in a much better position to identify patterns and respond to deficiencies in materials, equipment, or regulations.

**21. Adoption of a performance standard for the physical security of DMV facility, including whether DHS should adopt the ANSI/NASPO “Security Assurance Standards for the Document and Product Security Industries,” ANSI/NASPO-SA-v3.OP-2005, Level II as the preferred standard. DHS is considering the American National Standards Institute/North American Security Products Organization’s “Security Assurance Standards for the Document and Product Security Industries,” ANSI/NASPO-SA-v3.OP-2005, Level II, as the preferred performance-based standard for physical security of DMV facilities. DHS seeks comment on adoption of this standard, as well as recommendations on other appropriate performance-based standards to meet this statutory requirement. DHS also specifically seeks comment on the extent that the adoption of any performance-based standard would require modification of existing office space or construction of new space. DHS also seeks comments on the extent to which physical changes to existing office spaces required by the adoption of the ANSI standards or any other physical security performance-based standards would impact historical properties.**

AAMVA participated in the development of this standard by the North American Security Products Organization (NASPO) and is very familiar with it. The intent of this standard is to ensure security of commercial operations that manufacture secure products. There are significant differences between the way an open-to-the-public government entity, such as a DMV, and the way a closed-to-the-public commercial entity operates. Some parts of this standard, while costly, may prove effective for a DMV to specify as manufacturing security requirements for its vendors, but there are too many exceptions to make it useful for evaluating the operations of an open government facility. This direction would be extremely costly for DMVs, especially those that have geographically distributed facilities.

The NASPO standard should not be adopted for any DMV facility that produces driver’s licenses or identification cards. Every facility would need physical changes to comply with the NASPO standard. Many of these facilities are in old state buildings that have significant retrofitting issues and potential environmental (asbestos) issues if any part of the facility is disturbed. States also lease facilities and are locked into long term leases, where any change would be costly. It too should be recognized that some state

laws require counties or local county clerks to issue licenses and/or participate in the driver's license or identification card issuance. If the NASPO standard is followed, there would be considerable costs to local government as well.

The appropriate facility security standard needs to be developed in consultation with AAMVA members. DMVs have security provisions in place that address access, alarms and monitoring at the highest level as well as other covert security features. In order to answer the part of this question that deals with the extent of modification of existing office space or new construction, states would need to complete a costly facility assessment of all their facilities. AAMVA members would be happy to provide DHS with a tour of some state facilities to help the writers of the proposed regulations better understand the constraints and costs associated with facility changes. This proposed standard, coupled with the proposed directions for re-enrollment, renewals and replacements in the NPRM, could potentially force states to acquire all new facilities, break existing leases and completely change their issuance system and network. Compliance would literally be impossible.

**22. Whether the physical security standards proposed in this rule are the most appropriate approach for deterring the production of counterfeit or fraudulent documents, and what contractual issues, if any, the States will face in satisfying the document security requirements proposed in this rule.**

The recommended NASPO physical security standards are not appropriate and are misapplied to the DMV office environment. NASPO is an ineffective standard for the DMV's to use and its intent was not for high volume, high traffic customer environments. Its only potential application is to vendor production facilities. Vendors follow stringent standards similar to NASPO and are required to do so in their contracts with the DMVs. As noted, many states have made strides in the physical security of their issuance and production facilities. AAMVA members would like to work directly with DHS to develop a set of best practices in this area. Surely, the Department has physical security experts who could serve as resources to work with AAMVA and its members, and does not have to overlay a standard developed for other purposes. Until such a guidance document exists, states should continue to have the flexibility to determine what works for their issuance and production networks and outline such in their physical security plans to DHS as part of certification. Facility security is one component of ensuring a secure issuance process but it must work in concert with other components such as employee integrity, vendor/contractor reliability, systems reliability, process performance and control and law enforcement investigations. Fraud is a function of risk, people, processes, product and places. There is no single "silver bullet" deterrent. The extent of facility "protection" contemplated in the NPRM is excessive and only one element in an overall DMV risk management approach to deter production of counterfeit and fraudulent documents. In fact, in most instances, the cards are not counterfeit or fraudulent. They are real. The source documents are the underlying issue. On a daily basis, fraudulent documents are attempted to be used at DMVs. These documents (especially those issued by the federal government such as immigration documents and social security cards, and those issued by the states such as birth certificates) have long been a concern due to their lack of security features.

If in this question, DHS is referring to the card security standards, AAMVA members recommend that DHS use the AAMVA *Driver Licensing and Identification Card Design Specification* as the standard. The

standard, as proposed in the NPRM, could result in a less secure card as every state's card would have the same features and a compromise in one state could have national implications. AAMVA members as well do not support the use of one and only one substrate material for a driver's license or identification card.

States will face significant contractual conflicts if the document security standards in this NPRM remain in the final rule and if the time frames for implementation and re-enrollment are not changed. States are using the AAMVA *Driver Licensing and Identification Card Design Specification* as the model to prepare bid packages for new contracts or renewals. Contract periods for card vendors vary by state and are driven by procurement rules. One state, for example, has a contract in place for the next seven years. Most states have at least five year contracts. Again, it is recommended that DHS use the AAMVA *Driver Licensing and Identification Card Design Specification* as the minimum card security standard, allowing states to build on its provisions. States should not be expected to break or amend existing contracts and should not be expected to implement any changes to card security until their existing contracts expire.

**23. The potential environmental impacts of the physical security standards and other requirements proposed under this rule.**

AAMVA members contend that the NASPO facility standards are misplaced in the operation of a DMV, especially in over-the-counter issuance states with decentralized and distributed driver's license and identification card issuance networks. The physical security standards recommended in the NPRM and the aggressive, unworkable re-enrollment schedule will place insurmountable stress on issuance facilities in every state. Many of these facilities are not owned by the state or are shared facilities. Any time old, outdated facilities are retrofitted; there is the risk of environmental impacts like asbestos removal and abatement. These situations are not only costly but environmentally risky.

**24. DHS specifically requests comments on the federalism aspects of the background check requirements proposed under this rule.**

Recognizing that licensing is for the most part a state responsibility, the states should be able to have the flexibility to determine what, if any, background checks are completed and how they are applied to their employees. AAMVA members recommend that background checks be left to state discretion.

**25. DHS invites comment on whether the proposed list of disqualifying offenses is appropriate, too large, or insufficient as it concerns REAL ID.**

State DMVs understand DHS' desire to limit potential fraud in DMVs and with DMV contractors by ensuring that those who committed certain offenses are not permitted to be employed in DMVs or work under contracts with DMVs. AAMVA members believe that this federal intervention into what are effectively state personnel rules and hiring practices is misplaced. And, as stated previously, many of these issues must be part of the bargaining process with state unions or must comply with state personnel policies. States should be able to determine what, if any, disqualifying offenses are appropriate and should be able to do so within the confines of their individual state personnel policies. States will enumerate disqualifying

criteria in the state self-certification, as well as procedures for interim hiring pending results of background checks.

**26. What benchmarks are appropriate for measuring progress toward implementing the requirements of this rule and what schedule and resource constraints will impact meeting these benchmarks.**

There are far too many constraints to mention all those that will prevent states from meeting these proposed regulations and any proposed benchmarks. The menu of items includes:

- procurement practices
- process changes
- existing contractual arrangements that cannot be altered without significant penalty
- lack of funds
- lack of legislative authority
- lack of personnel
- facility constraints
- computer system changes
- lack of new verification systems
- lack of reliable existing verification systems

Those are only some of the constraints. Strategies to address these constraints can be used for measuring progress toward implementation. AAMVA members remind DHS that many of the noted items are critical path items and control often does not rest with the DMV. AAMVA members recommend that the Department focus on setting a realistic implementation and re-enrollment timetable before any benchmarks are established. Items, like other federal mandates and state legislative initiatives as well as major system development projects are also constraints to implementing P.L. 109-13.

**27. Whether DHS should standardize the unique design or color required for non-REAL ID under the REAL ID Act for ease of nationwide recognition, and whether DHS should also implement a standardized design or color for REAL ID licenses.**

The AAMVA *Driver Licensing and Identification Card Design Specification* does not require a similar color for all states, and it allows for unique designs to recognize that driver's license and identification card issuance is a state process. It does, however, standardize the application of security features to address card security threats. AAMVA members believe that DHS should not standardize a unique design or color for non-REAL ID credentials or REAL ID credentials. AAMVA members do recommend that the branding, however, be transferred to the REAL ID credential instead of the non-REAL ID credential. This requirement definitely would lead some individuals to believe this is a step on the road to a national ID card.

## **REAL ID ACT CLARIFICATIONS STILL NEEDED**

As noted in the introduction to this response, there remain a number of specific clarifications that need to be provided by DHS. AAMVA members have addressed many of those questions in the specific NPRM sections. In addition, AAMVA members request clarification on the following:

1. Does the definition of a REAL ID driver's license and identification card take into consideration an interim type of driver's license or identification card for states that issue permanent driver's licenses and identification cards through a central issuance process? What are the security requirements for an interim license and will an interim driver's license or identification card be acceptable for "official purposes"? AAMVA members recommend that DHS amend the language of the proposed rule to expressly state whether an interim driver's license or identification card issued by a state using a central production facility for the manufacturing of driver's licenses and identification cards would be acceptable for use at a federal facility, to board a federally-regulated commercial aircraft or enter a nuclear facility. As many states may be moving to central issuance and issuing interim cards, AAMVA members ask DHS to set circumstances under which such a document could be accepted.
2. AAMVA members request DHS to advise what, if any, security features would be required on interim cards issued by states that employ central issuance. DHS should recognize that any additional features would increase the potential cost of interim cards. There remain very real circumstances where interim cards are the only form of identification citizens may have in their possession.
3. The NPRM is silent on a long-standing practice in some states that allow the issuance of both a driver's license and identification card to the same individual. This practice allows customers to travel with an identification card and not risk the loss of their driver's license. As well, this practice is a revenue generator for states. AAMVA members recommend that this continue to be a state decision.
4. DHS uses the terms verification, authentication and validation interchangeably in the NPRM. DHS needs to define what its expectations are regarding those terms as part of the definitions section of the NPRM. AAMVA members will be happy to assist DHS in clarifying these terms.
5. DHS need to clarify specifically at what age a REAL ID is to be issued. Some states issue identification cards to children as young as 10 years old and some begin the licensing process at under age 16.

## **NPRM INCONSISTENCIES**

P.L. 109-13 stipulates that a "State must refuse to issue a driver's license or identification card to a person holding a driver's license issued by another State without confirmation that the person is terminating or has terminated the driver's license." Yet the NPRM notes that in subsection (c) prior to issuing a **REAL ID**

driver's license or identification card, States must check with all other States to determine if any State has already issued a **REAL ID** driver's license or identification card to the applicant. It further notes in section (1) If the State receives confirmation that the individual currently holds a **REAL ID** driver's license or identification card issued by another State, the receiving State must: (i) Take measures to confirm that the person has taken steps to terminate, or has terminated, the **REAL ID** driver's license or identification card issued by the prior State, (ii) Require the person to surrender the **REAL ID** driver's license or identification card issued by another State unless the person signs a declaration under penalty of perjury pursuant to 28 USC 1746 stating that the driver's license or identification card was lost or stolen. (Emphasis added)

If intentional, this inconsistency effectively defeats the one driver, one record goal of the REAL ID Act and is detrimental to highway safety. Any all-driver system should function for compliant and non-compliant driver's licenses and identification cards and all states should be able to use it if they implement the REAL ID Act or not.

AAMVA members also note that in Section 37.15 (f) (ii) of the NPRM regarding physical security features for the driver's license and identification card, the regulation reads: "As part of the State's initial and annual certifications, the State must submit to DHS results from a facility described in paragraph (g)(2)(i) of this section, in the following areas: (A) Photo substitution. (B) Delamination and deconstruction. (C) Reverse engineering. (D) Modification of any data element. (E) Erasure of information. (F) Duplication, reproduction, or facsimile creation. (G) Effectiveness of security features (three levels). (H) Confidence and ease of second level authentication." There is no (g)(2)(i) section in the NPRM. This must be clarified.

## CONCLUSION

The driver's license and identification card issuance process in all DMVs is complicated and critical to their mission. States have improved the security of their cards, they have improved processes surrounding driver's licensing and identification card issuance and they have taken steps to significantly deter internal and external fraud and abuse. AAMVA members urge DHS to use the *Driver's License and Identification Card Security Framework* that AAMVA members and other experts developed with the support of the US DOT. DHS is also urged to use the *Driver's License Agreement* which was also provided to the agency as a reference document as it too was developed by jurisdictional experts in cooperation with the US DOT. Finally, AAMVA members urge DHS to use the recommendations provided in the *REAL ID National Impact Analysis* prepared by AAMVA, NCSL and NGA. This analysis was completed through an extensive survey of all the states with 47 of 51 jurisdictions, representing nearly 90 percent of all US driver's licenses and identification cards issued, responding. All of this material is the work of experts in driver's licensing and identification card issuance. There is no need to reinvent the wheel.

About 100 years ago, states began to issue driver's licenses to address one basic tenet; to attest to a person's ability to drive. Those tenets have certainly changed over the years and the pure safety and driver credentialing mission has been distorted by many federal mandates and ancillary requirements. The federal government requires DMVs to be responsible for such on driver related functions as driver license suspensions for parents not paying court-ordered child support and for voter registration with "motor voter." A host of other mandates are required by various state laws. And, most recently DMVs are responsible for

the evolving tenet of the use of the driver's license and identification card as the most commonly accepted form of identification in the U.S.

AAMVA's members are used to change and challenge and adapting rapidly. AAMVA members are supportive of the concept of the REAL ID Act and its most basic intentions to continue to secure the driver's license and identification card issuance process and to advance minimum standards. However, while providing some flexibility to the states, this NPRM impedes any state's ability to continue to make progress to secure the driver's licensing and identification card issuance process in a diligent and reasonable manner.

Despite the "flexibility" provided in the NPRM, many critical concerns remain for AAMVA members. Even with the "delayed" implementation and "phase-in" period for re-enrollment, visits to state motor vehicle agencies will increase over 75 percent annually. Implementing this NPRM will require additional staff, facility changes, additional training, system and process changes and the connection to systems that have yet to be developed. Every state faces its own unique set of challenges for implementation from different demographic, operational, legislative, technological and fiscal perspectives. Looming over all the implementation challenges, remains the fact that, even with the "extended" implementation deadline to December 31, 2009 and the date forward re-enrollment deadline to May 11, 2013, there still is simply not sufficient time to implement the requirements as contemplated in this NPRM.

AAMVA members recognize that REAL ID, if implemented, will need to be carefully considered in segments for both DHS and the states. Prioritization and value decisions based on risk and risk mitigation will need to be made over a period of time. As this process progresses, AAMVA members recommend that DHS focus on those items that can continue to reduce driver licensing and identification card fraud and assist the states in these efforts. AAMVA members recommend that DHS work with the states to strategically consider stages and a phased approach that focuses on risk based considerations that have value to improving the credential issuance process and reducing fraud. And, AAMVA members recommend that as this rulemaking process continues that DHS focus on establishing outcomes for the Act versus prescriptive requirements that are difficult to uniformly apply to more than 51 jurisdictions.

States have been and remain committed to increasing the security and integrity of their driver's license and identification card issuance processes. AAMVA members look forward to working with DHS beyond this initial NPRM.

AAMVA members strongly suggest that the next step in this rulemaking process not be the final rule this summer. With still so many uncertainties, with DHS' continued lack of clarity on many items, and with nearly 30 questions for additional input to the NPRM, AAMVA members recommend that DHS further extend the deadlines for implementation and re-enrollment and issue a second Notice of Proposed Rule Making this summer to allow states and other interested parties an additional opportunity to comment on changes that have been incorporated through this initial comment period.

While AAMVA members are cognizant of the critical need to continue to improve the driver's license and identification card issuance process and reduce fraud, DHS must recognize that the implications of

The Honorable Michael Chertoff

Page 53

May 1, 2007

implementation are far reaching. Many of those implications have not been adequately addressed in this NPRM. Applicant processing time will more than double for citizens in most states and wait times in some states will increase by up to 200 percent. The costs are astronomical. While the intentions are important, the Administration, DHS and Congress have continued to grossly underestimate the impact of the REAL ID Act.

AAMVA members recognize that there are many competing stakeholders who have specific interests in this NPRM. It is evident that DHS did consider and promulgate some of the AAMVA-NGA-NCSL recommendations to help operationalize the Act. However, as noted in this response, many key recommendations were not included. Therefore many of the provisions remain concerning and unworkable in the "real" motor vehicle world where customers meet the counter.

The most concerning provisions of the NPRM to AAMVA members are still consistent with the concerns verbalized by AAMVA/ NCSL/NGA in September 2006, well in advance of the NPRM publication in March 2007. Issues such as state-borne excessive costs for a federal mandate, an unrealistic implementation timeframe, a similarly unrealistic re-enrollment timeframe, lack of existent and reliable verification systems, prescriptive card design specifications and excessive physical security standards remain huge issues.

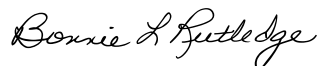
AAMVA members are confident that DHS will take these noted issues seriously and make necessary adjustments to the proposed regulations that will help the states continue to make improvements to the driver's license and identification card issuance process in a deliberate and sensible manner.

DHS has most recently and in the past recognized the expertise of AAMVA members and we are hopeful that it will do so in the future. AAMVA's members have made great strides in improving the driver's license and identification card issuance process and in improving identification security since that dreadful day on September 11, 2001. They remain poised to continue to do so in the future.


Sincerely,



Debra A. Hillmer, Chair of the Board, AAMVA  
Director, South Dakota DMV



Bonnie Rutledge, Chair, REAL ID Steering Committee, AAMVA  
Commissioner of Motor Vehicles, Vermont



Michael R. Calvin  
Interim President and CEO, AAMVA