October 15, 2023

Docket Management Facility,
U.S. Department of Transportation,
1200 New Jersey Avenue SE,
West Building, Room W12-140,
Washington, DC 20590-0001

AAMVA Comments on Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses [Docket No: TSA-2023-0002]

The American Association of Motor Vehicle Administrators (AAMVA) thanks the department of Homeland Security for the opportunity to comment on its proposal to amend the REAL ID regulations to waive, on a temporary and State-by-State basis, the requirement that mobile or digital driver's licenses or identification cards be compliant with REAL ID requirements to be accepted by federal agencies for official purposes when full enforcement of the REAL ID Act and regulations begins on May 7, 2025. As DHS is aware, the States have invested significant resources and time in developing the next generation of identity management products to fulfill its obligations in protecting its constituents' data and advancing identity protections in a mobile environment. With identity protection and constituent services at the forefront of our organizational mission, AAMVA offers the following comments to the docket.

IN GENERAL

Phased Approach

The department has indicated that this proposed rule is part of an incremental, multi-phased rulemaking that will culminate in the promulgation of comprehensive requirements for State issuance of REAL ID compliant mobile driver's licenses and mobile identification cards. AAMVA appreciates and supports the efforts to provide a temporary solution, provided on a case-by-case basis of waiving the requirement that a mDL be REAL ID compliant in order to be acceptable for federal official purposes. This will allow the use of implemented solutions through the May 7, 2025 enforcement deadline and provide states with a preliminary process to accommodate mDL innovation. While AAMVA provides additional comments regarding regulatory timing in conjunction with the enforcement deadline, AAMVA encourages DHS to consider that publication of this rule may occur too close to the deadline or after the enforcement deadline. AAMVA encourages DHS to consider a grandfather clause for those states whose mDLs are already accepted by TSA prior to the enforcement deadline.

Conditions for TSA Acceptance

The conditions for acceptance by TSA have been established as follows:
1) the mDL holder has been issued a valid and unexpired REAL ID compliant physical driver's license or identification card from the same state that issued the mDL
2) TSA has determined the issuing State to be REAL ID-compliant; and
3) TSA has issued a wavier to the State.

Given that TSA acceptance is dependent on the agency determining the issuing state is REAL ID compliant, AAMVA requests clarification on whether this is applicable to a one-time determination, whether the DHS schedule for re-

certification in the program is applicable, or whether the determination by DHS will be based on the State being in "good standing" via DHS program review at the time of State application for acceptance to DHS.

Definitions

AAMVA appreciates that TSA explains on page 60057 that –
"The definition of 'mDL' as used in this rulemaking is limited to the REAL [sic ID] Act and regulations and should not be confused with 'mDLs' as defined by other entities, or with State-issued mDLs that are not intended to comply with the REAL ID Act."

This clarification could potentially prove important in deciphering TSA's intent in some of the more complex areas of the proposed rule. Consistency in this application becomes complicated as the states seek clarity on the requirements TSA applies to acceptance in the waiver program and the agency's own intended use of the mDL specific to its official purposes (e.g. for air travel).

Clarification on Non-Compliant mDLs and Waiver Eligibility

Without reservation, AAMVA's largest issue lies with the language provided in amended §37.7(b)(3) of the proposed rule, which states (on page 60085):

"(b) State eligibility. A state may be eligible for a waiver only if, after considering all information provided by a State under §37.10(a) and (b), TSA determines that –
"(3) The State issues mDLs only to individuals who have been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card issued by that State."

The language used here would disqualify a large number of states that issue non-REAL ID compliant credentials and mDLs from participation in the TSA waiver program. While states may issue non-REAL ID compliant credentials, the states supply differentiation between compliant mDLs and non-compliant mDLs much as they would for any physical card. Given TSA is currently already accepting mDLs from states that issue both compliant and non-compliant credentials, AAMVA would presume the purpose of the waiver program is to extend the acceptance of the mDLs in the lead to the full enforcement date and not curtail their use. Differentiation of compliant versus non-compliant is already a feature of most mature mDLs. As something being built as standard to the mDL, AAMVA would assume that TSA would be able to accept and view the flag as pushed to reader to make security determinations and not limit waiver applications based on this language.

As written, this language would also present serious equity and social issues. Unless corrected, this language could disenfranchise very specific demographics from participation in mDL programs more widely. As TSA itself states, "This iterative rulemaking approach supports Executive Order (E.O.) 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government), by using 'technology to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States.'" But as written, the language is exclusive and accomplishes the opposite of Executive Order 14058.

AAMVA is unclear on whether this is simply a typo, a misinterpretation or intentional. AAMVA would recommend inclusive language more along the lines of, "(3) The State issues mDLs in a manner consistent with the way it issues physical credentials in that the mDL must set the "DHS compliance" data element (see 37.10) to reflect whether the credential is compliant with the REAL ID program and the State may only issue a REAL ID compliant mDL to an individual that qualifies for a REAL ID compliant credential."

The States must preserve the ability to both issue non-compliant credentials and mDLs and simultaneously be eligible for temporary waiver application to TSA for this to be an effective rule. If the language is intended to exclude

states from eligibility if they issue non-compliant products, this would result in numerous states being ineligible for this program - significantly reducing the benefits of accepting mDLs and causing confusion for both TSA staff and the general public.

Enforcement Date Forward Acceptance of mDL for Official Purposes and Differentiation of Application to the Waiver Program

On page 60059, TSA states that –
"An mDL cannot be REAL ID-compliant until TSA establishes REAL ID requirements in regulations and States issue mDLs compliant with those requirements. As a result of this requirement, mDLs must also be REAL ID-compliant to be accepted when card-based enforcement begins on May 7, 2025."

AAMVA requests that TSA clarify two distinctions:

1) that while final regulations may not have been prescribed providing for the standards and requirements a state must meet to have an mDL be certified as REAL ID compliant that a state may still apply for, and be approved, to participate in the waiver program this proposed rule contemplates up to, and extending beyond, the May 7, 2025 enforcement date once approved by TSA. With final mDL regulations years out, differentiation between full mDL REAL ID compliance and sufficiency for participation in TSA-approved mDL acceptance are two distinct things that are understood by the states. Eliminating acceptance after the full enforcement date and before the rule is published would handicap both the enrollment process and the ability for TSA to streamline travel efficiencies gained by state investments in mDL issuance.

2) That a state that issues both compliant and non-compliant driver's licenses (and therefore corresponding mDLs that match the physical credential) are not limited in the products presented to TSA for official purposes. State mDLs currently carry REAL ID flags that can be conveyed for sufficiency determinations by TSA security staff. While this may not be sufficient independently for air travel after the final enforcement date, a state may still apply for and be granted access to the waiver program if they issue both compliant and non-compliant mDLs and credentials.

Prescription of Technology Solutions
On page 60061, TSA states that, "Based on its analysis of the current environment, TSA believes that States are issuing mDLs using widely varying technology solutions, resulting in a fragmented environment rather than a common standard for issuance and use." AAMVA notes that while there may be variations in technology solutions, the adherence to the standards are what is most important as varying technologies can continue to conform to the same standard. This approach allows flexibility in vendor and approach while still promoting interoperability and security. AAMVA only notes that the two are not mutually exclusive. AAMVA notes that it is currently encouraging adoption of these standards by requiring states that are joining its Digital Trust Service (DTS) to support ISO/IEC 18013-5.

Incorporations by Reference
AAMVA thanks TSA for its inclusion of its *Mobile Driver's License (mDL) Implementation Guidelines Version 1.2* as the primary resource for incorporation by reference in 6 CFR §37.4.

While minor, and potentially semantic, AAMVA does not consider its Guidelines "more stringent" as described on page 60062. AAMVA does qualify 18013-5 by limiting some of the options for issuers and making some fields that are optional in 18013-5 mandatory. However, we do not consider this as "more stringent" but an example of how AAMVA has expanded the ISO data set as allowed in 18013-5.

Time Period of Waiver Authority

TSA states on page 60067 that "Any temporary waiver issued by TSA would be valid for a period of 3 years from the date of issuance. The waiver enabled by this rulemaking would be repealed when TSA publishes a Phase 2 rule that would set forth comprehensive requirements for mDLs." AAMVA urges TSA to consider appropriate transition periods for the development of state-based mDL solutions. There may be a very urgent need for the waiver authority granted by TSA to extend beyond the publication of its phase 2 rulemaking as states transition their technology to accommodate the new technology requirements associated with the new rule. While it is hard to anticipate exactly what the grace period may be, AAMVA urged TSA to avoid dictating that the authority of the waiver would expire immediately upon publication of the phase 2 rule.

TSA Provision of Guidance
AAMVA thanks TSA for the advance provision of its "Mobile Driver's License Waiver Application Guidance" to assist states that are considering applying for a waiver.

Extenuating Circumstances Associated with mDL Acceptance
AAMVA understands the need for TSA to caution that "the waiver granted by this rulemaking does not represent a commitment by Federal agencies to accept mDLs issued by a State to whom TSA has granted a waiver." AAMVA is understanding of the fact that there may be a need to suddenly halt acceptance for reasons beyond the agency's control, such as suspension or termination of a waiver, technical issues with IT systems, or a loss of resources to support mDLs. In such instance, we further understand that there may be instances where individuals are denied use of an mDL for official purposes, including boarding aircraft. AAMVA urges DHS to consider the implications of such disruptions and contemplate whether there may be utility in providing support and communication of these types of events either at the security checkpoints themselves or more globally through the TSA website where any disrupting status effects that may impact the state-issued mDL eligibility might be shared in advance of travel plans or detailing the reasons why the credential may not be sufficient. The states themselves will not be positioned to advise on behalf of TSA, and TSA alone will be the knowledgeable source on current status of waiver eligibility or IT issues impacting acceptance. AAMVA encourages TSA to consider any needed support or additional resourcing associated with waiver or mDL acceptance and disruption. For instance, as part of the requirements for federal agencies that accept mDLs, TSA stipulates that agencies would make confirmation of state eligibility by verifying that the State's name appears in a list of States to whom TSA has granted a waiver published on www.dhs.gov/real-id/mDL. This could also be a place to publish disruption information.

Specific Questions

1. Applications for waivers. Provide comments on:
a. The estimated cost and time required for States to complete and submit applications for waivers, including the initial mDL waiver application, resubmission and reapplication;

AAMVA defers all estimates on cost and administrative burden hours to its state members who are more directly involved with pricing criteria, program and geographic differences, and availability and cost of resources.

b. The estimated number of State and territories that would submit a waiver application and when those States and territories would submit a waiver application;

AAMVA would assume this is an evolving demographic. The states that are already pursuing mDL solutions would be first to submit an application package, but there are numerous others that are studying and expanding their mDL and digital identity footprint. The utility of providing this data today may not sufficiently represent the number pursuing a wavier application by the time this rule is finalized. TSA lists a number of states that are both actively pursuing and well enroute on page 60061 of the proposed rule.

c. The percentage of States that would receive a decision of approved, insufficient, or denied;

Given TSA makes the ultimate determination on whether a State is approved, insufficient or denied, AAMVA is hard pressed to make a projection on TSA determinations.

d. The percentage of States receiving a decision of insufficient that would resubmit an amended application;

AAMVA would imagine that many, if not all, states would pursue additional clarification on why their application is worthy of TSA consideration for waiver.

e. The assumption that TSA would approve all resubmitted applications.

AAMVA would consider it reasonable that if a state meets the criteria of the proposal and is worthy of consideration that TSA provide due consideration and approval where warranted. AAMVA would defer to its members on quality of application, but would assume that there may always be instances where an application may require additional clarification or be subject to additional scrutiny.

2. Application Criteria. Provide comments on:
a. The costs State may incur to demonstrate compliance with the criteria to apply for a waiver as required by proposed §37.10(a) and appendix A to subpar A of the part, including the costs and availability of any professional services required;

AAMVA defers all estimates on cost and administrative burden hours to its state members who are more directly involved with pricing criteria, program and geographic differences, and availability and cost of resources.

b. The appropriateness of the application requirements set forth in proposed §37.10(a) and appendix A to subpart A of the part;

AAMVA welcomes the discretion provided as part of the application, including the advance provision of guidance and examples that may assist the states in making a sufficient, successful application. With that in mind, AAMVA offers the following comments on Appendix A:

With respect to references, many requirements require “full compliance” with references (e.g. the CA Browser Forum documents) without specifically pointing to the specific parts of these documents that are applicable, or qualifying the documents as needed to apply to the mDL environment. This creates uncertainty for both Issuing Authorities and auditors on what the actual requirements are.

For example:

- Many requirements refer to the “CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” as a whole (1.1, 1.2, and 1.3, to name but a few). However, Section 1.1 of this CA/B document states the following: “These requirements only address Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing… may be covered in future versions.” Section 1.2 also states: “This certificate policy (CP) contains the requirements for the issuance and management of publicly-trusted SSL certificates…”. It could therefore be argued that since Issuing Authorities do not issue SSL certificates intended to be used for authenticating servers accessible through the Internet, and that signing a mDL is much closer to signing code than it is to issuing a SSL certificate intended to be used for authenticating servers accessible through the Internet, the requirements of the document do not apply, at least not verbatim.
- Requirement 1.1 in Appendix A requires an Issuing Authority to maintain a Certificate Policy in full compliance with, among others, the “CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” as a whole. This introduces several uncertainties, including:

- Section 2.2 of the CA/B document requires an Issuing Authority shall make revocation information available in accordance with its policy. Given that Requirement 1.1 only addresses the maintenance of a Certificate Policy itself, what is the Issuing Authority's responsibility in respect of the publication of revocation lists?
- Section 2.2 of the CA/B document requires an Issuing Authority to publicly disclose its Certificate Policy and/or Certification Practice Statement. Given that Requirement 1.1 only addresses the maintenance of a Certificate Policy itself, what is the Issuing Authority's responsibility in respect of a Certification Practice Statement?
- Section 2.2 of the CA/B document requires an Issuing Authority's Certificate Policy to state its policy or practice on processing CAA records. This arguably does not apply to an Issuing Authority that only issues document signer certificates for its own use. Yet the Issuing Authority is required to maintain its Certificate Policy in full compliance with the CA/B document.
- Section 2.2 of the CA/B document requires Issuing Authorities to allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. This arguably does not apply to the mDL environment where Issuing Authorities distribute only their root certificates. Yet the Issuing Authority is required to maintain its Certificate Policy in full compliance with the CA/B document.
- Section 3.2.2 of the CA/B document states requirements on authentication of organization and domain identity. This arguably does not apply to an Issuing Authority that only issues document signer certificates for its own use.

While it would be an option for Issuing Authorities to just indicate, in its Certificate Policy, which requirements from the CA/B document do not apply, such a determination would be based on the opinion of the Issuing Authority. Different Issuing Authorities could make different determinations even though the facts may be the same.

- Requirement 1.1 in Appendix A requires an Issuing Authority to maintain a Certificate Policy in full compliance with, among others, the "CA Browser Forum Network and Certificate System Security Requirements" as a whole. This document appears to contain very specific network and certificate administration requirements (many of which are covered by items in Appendix A), and does not address requirements on a Certificate Policy. It is therefore unclear how a Certificate Policy can be in full compliance with this document.

AAMVA requests that TSA be specific when referencing other documents on exactly which parts apply.

2.2: The terms "privileged account" and "service account" is not defined in the rule. The terms also are not defined in any of the references. Please define these terms.

4.1: It is not clear how "coordination among State entities" applies to a policy to control insider threat security risks. Please clarify.

4.1: The policy to control insider threat security risks is required to comply with "all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines". Absent a list of "all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines" it will be impossible for an auditor to determine if an Issuing Authority's policy complies with this requirement.

4.7: It is surmised that training item 2, "Authentication and vetting policies and procedures", applies to Issuing Authorities that issue certificates to other entities (as described in the "CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"). Since an Issuing Authority in the mDL context

does not issue document signer certificates to anyone other than the Issuing Authority itself, training in respect of authentication and vetting policies arguably do not apply.

5.4: It is not clear whether "dedicated" requires the HSMs to be dedicated to root certificate private keys, and/or dedicated only to the Issuing Authority. Please clarify. In addition, it is not clear if this rules out a HSM that physically supports more than one State but is logically divided into segments that each is under control of the State it services (or of a delegated third party).

c. The impact that the Initial Public Versions of Revision 4 of NIST SP 800-63, NIST SP 800-63A, NIST SP 800-63B and NIST SP 800-63C may have on the requirements set forth in proposed §37.10(a) and appendix A to subpart A of the part, including States' ability to demonstrate compliance with the criteria to apply for a waiver as required by proposed §37.10(a) and appendix A to subpart A of the part.

AAMVA has submitted formal comment to NIST via a comment template. AAMVA is happy to furnish these comments to TSA upon request.

3 Audit report. Provide comments on requiring States to submit a report of an audit as required in proposed §37.10(b), which report would require verifying the materials that a State would provide in its application for a waiver as required by proposed §37.10(a), including:
a. The appropriateness of requiring an audit to be conducted by a recognized independent entity;

While AAMVA appreciates the necessity for having an independent auditor review the state's mDL processes, we urge that the audit be as broadly based as possible and be provided as an option to the state's submitted application. The states well understand that independent evaluation is helpful, but some states may be better positioned to provide resources towards an independent evaluation where others may have more difficulty. In the hopes of providing an equitable evaluation across all jurisdictions, AAMVA questions whether the application process itself should prove sufficient in and of itself and that any additional clarity may be provided by a state directly to TSA instead of a third party evaluator (but not be required). TSA may include this in its "Mobile Driver's License Waiver Application Guidance" but not require this of every applicant.

Additionally, AAMVA notes that in its mDL Guidelines, the organization differentiates between requirements for which self-certification is sufficient, and those for which independent expert certification is required. In short, independent expert certification is required for items that are highly technical and for which knowledge to assess is unlikely to exist within a state. AAMVA recommends that TSA consider following a similar approach, combining independent expert certification as a substantiating element to the application and considered alongside any self-certifications that may be already presented to DHS (such as those required in conjunction with REAL ID).

b. The appropriateness of requiring an auditor to hold an active Certified Public Accountant license in the State that is seeking the waiver;

AAMVA encourages TSA consider very carefully whether this be a requirement of submission as described above. If it is, AAMVA wonders whether credentials more closely aligned to certification of systems management, ethics, and business practice might be worthy examples in addition to the holding of a Certified Public Accountant license in the State. It should be noted that laboratories that check compliance with 18013-5 are typically not CPAs. Given all of these may be relevant, instead of the requirement that a specific license be held, that the reviewing auditor simply be listed if one is used as part of the application process.

c. The appropriateness of requiring an auditor to be experienced with information systems security audits, including whether such auditors should have different or additional experience;

See above.

d. The appropriateness of requiring the auditor to be accredited by the State seeking a waiver.

See above.

e. The appropriateness of requiring an auditor to hold a current and active American Institute of Certified Public Accountants (AICPA) Certified Information Technology Professional (CITP) credential or ISACA (F/K/A Information Systems Audit and Control Association) Certified Information System Auditor certification;

See above.

f. The availability of auditors who meet the criteria specified in proposed §37.10(b)(1);
AAMVA is unaware of current state certification data for each of these classifications.

g. The estimated cost and time incurred by States to obtain a report by the auditor;

AAMVA defers all estimates on cost and administrative burden hours to its state members who are more directly involved with pricing criteria, program and geographic differences, and availability and cost of resources.

4. DHS Mobile Driver's License Waiver Application Guidance comments;

Please see previous AAMVA comments on the DHS Mobile Driver's License Waiver Application Guidance. This includes consideration of the incorporation by reference being published here rather than in the rule for ease of modification as well as comments regarding privacy protections described in §37.10. AAMVA provides additional related comments in its answers to question 2(b) above.

5. Waiver validity period, DHS is considering a three-year validity period for waivers. Provide comments on the appropriateness of a three-year validity period for waivers and on alternate validity periods.

AAMVA notes that the period of validity to the waivers should directly correlate with the amount of time the States indicate it would take to submit a sufficient application and receive response from DHS. Given some of the dependence on waiver validity period will rely on DHS' ability to turn around applications from numerous states simultaneously, AAMVA encourages DHS to make the eligibility period for the waivers sufficient that the states are not constantly submitting renewal submissions and waiting on DHS to make determinations on their state. Further, given that the conditions for granting of eligibility of the waivers is dependent on the State being deemed REAL ID compliant by DHS, the period of eligibility should also be sufficient such that it covers both DHS's review of the specific waiver application as well as the certification of the State's REAL ID program generally. AAMVA also encourages TSA to review its previous comments regarding how the validity period straddles the final REAL ID enforcement deadline of May 7, 2025.

6. Mobile driver's license readers. Provide comment on the costs to procure mDL reader equipment, estimated reader usage by Federal agencies, States, and businesses and the functional form of such reader equipment.

AAMVA defers comment to its state members and federal agencies regarding reader procurement.

7. mDL acceptance. Provide comment on the number of federal agencies other than TSA DHS and DHS component agencies that voluntarily choose to accept mDLs for official purposes for identity verification, including:
a. The number and types of locations where mDLs will be accepted;

AAMVA defers visibility on federal agency use of credentials for official purposes to the federal agencies granted authority to securely vet visitors for those official purposes.

b. the number of individuals that are expected to obtain mDLs.

AAMVA defers comments on licensing numbers and the percentage of individuals who opt for an mDL credential to the states. FHWA periodically provides general licensing data as reported from the states, but it does not include the number of individuals opting for a mDL credential.

8. Costs to individuals. Provide comment on costs incurred by mDL users, including costs associated with obtaining an mDL.

AAMVA defers all estimates on cost and administrative burden hours to its state members who are more directly involved with pricing criteria, program and geographic differences, and availability and cost of resources.

9. TSA invites public comments on Alternative 4, including, but not limited to, costs to the affected entities to comply with the minimum standards, benefits of the alternative compared to the preferred alternative, and risks to security and privacy of accepting mDLs based on the minimum requirements.

AAMVA defers all estimates on cost and administrative burden hours to its state members who are more directly involved with pricing criteria, program and geographic differences, and availability and cost of resources.

Under alternative 4, TSA would first establish minimum requirements for issuing REAL ID compliant mDLs before TSA later sets more comprehensive requirements as additional guidance and standards become available in the mid and long term. However, there is a lack of clarity on how this sufficiently differs from the proposed rule. AAMVA understands that under the alternative, the standards would be codified – but given the potential for standards to change or be modified, codifying the standards can be more cumbersome than incorporation by reference. If the issue is where the "requirements" currently published in the Waiver Application Guidance should be published, AAMVA would recommend that rather than burdening the incorporation by reference in the rule itself, it should instead be incorporated into the Guidance document itself, which lends itself to much easier changes to version and most current standard and reference.

AAMVA may need additional clarity on the distinction between these two alternatives if this is not the question being posed by TSA.

§37.4 Incorporation by Reference

In general, referring to dated documents is understandable. However, it also creates problems given the relatively fast pace with which standards often get updated, and the relatively slow pace with which regulations adapt. It may be an option to refer to the most recent version of these documents rather than to specific versions.

§37.7 Temporary waiver for mDLs; State eligibility
See previous comment AAMVA supplied in the section entitled "**Clarification on Non-Compliant mDLs and Waiver Eligibility"** provided above. These comments are crucial to the success of the rule.

§37.8 Requirements for Federal agencies accepting mDLs issued by States with temporary waiver
Under this section, federal agencies must confirm the state holds a valid certificate of waiver consistent with §37.7(a) by verifying that the State appears in a list of mDLs approved for Federal use, available as provided in §37.9(b)(1). AAMVA reiterates that support for disruption to the site, or to the ability to verify via website be established and in place prior to the federal agency requirements. While the web site will be helpful in almost all

instances, a support mechanism should be in place if the site were unavailable to certain airports, staff, etc. so that the waiver remains valid.

§37.10 Application criteria for issuance of temporary waiver for mDLs; audit report; waiver application guidance.

See AAMVA's previous comments regarding the audit process under its answers to "specific questions" above.

37.10 (a)(1)(i): An mDL holder's PII is already stored on state systems for purposes of complying with the existing REAL ID rule. AAMVA has concerns that the wording as provided under this section may introduce additional requirements, unrelated to mDL issuance, on states that go beyond current program requirements. AAMVA advises against expanding the tenants of the REAL ID program through this rulemaking.

37.10 (a)(1)(iii, iv, v and vi): The ostensible goal of these items are to ensure that an mDL is provisioned to the rightful mDL holder's device. It should be noted that this binding has no value to a relying party at transaction time. In in-person use of a mDL, the relying party matches the holder (or more accurately, the presenter of the mDL) to the portrait image in the authenticated mDL data. Other than protection against copying of an mDL, which is built into the authentication protocol and is independent from whether or not the provisioning was to the rightful mDL holder's device, and in the absence of requirements for the device to bind to the rightful mDL holder at transaction time, at transaction time the relying party cannot place any trust in the holder's device or in the association between the mDL holder and the device. AAMVA questioned why TSA, as a relying party, would place requirements on an Issuing Authority that arguably do not affect TSA.

37.10 (a)(3): Privacy is an important consideration. It mostly applies to the agreement between an mDL holder and an Issuing Authority. The only extent to which it may apply to TSA is that TSA may want to ensure it does not receive more information than was requested. It is therefore recommended that TSA update this requirement such that States are only required to provision mDL applications that, at transaction time, will not release more data than TSA requests. Additional privacy requirements, while important to both States and mDL holders, arguably do not affect TSA.

37.10 (a)(4): There is a reference to v. 1.1 of the AAMVA mDL Implementation Guidelines. It is surmised that this reference should be to v. 1.2, the only version that is included in 37.4.

37.10 (a)(4)(i): The "resident address" is defined as a mandatory data element in the AAMVA mDL Implementation Guidelines v. 1.2, and not as an optional data element as noted here.

37.10 (c)(2): It will be very helpful if each row in the Waiver Application Guidance notes the requirement in the rule that it addresses.

AAMVA thanks TSA for undertaking this rulemaking to facilitate interstate commerce, serve the United States constituency in a modern, more secure manner, and keep pace with the expectations of the traveling public. AAMVA looks forward to continued collaboration on this rulemaking and stands ready to assist TSA wherever possible.

Cian Cashin
AAMVA Director of Government Affairs
ccashin@aamva.org