# AAMVA DL/ID Security Framework

A Package of Decisions Based on Best Practices, Standards, Specifications and Recommendations to Enhance Driver's License Administration and Identification Security

AAMVA

American Association of
Motor Vehicle Administrators

DISCLAIMER:

AAMVA, a non-regulatory organization, uses its membership's expertise to develop standards, specifications and best practices to foster the enhancement of driver licensing administration and identification security.

AAMVA determined the need for a comprehensive framework of minimum requirements with enhanced recommendations to improve the quality, reliability, uniformity and security of the driver licensing process in North America.

Throughout this document, AAMVA uses the word "shall" where it believes all jurisdictions "need" to adhere to the proposed requirements for maximum effectiveness.

# Table of Contents

# 1.0 Overview

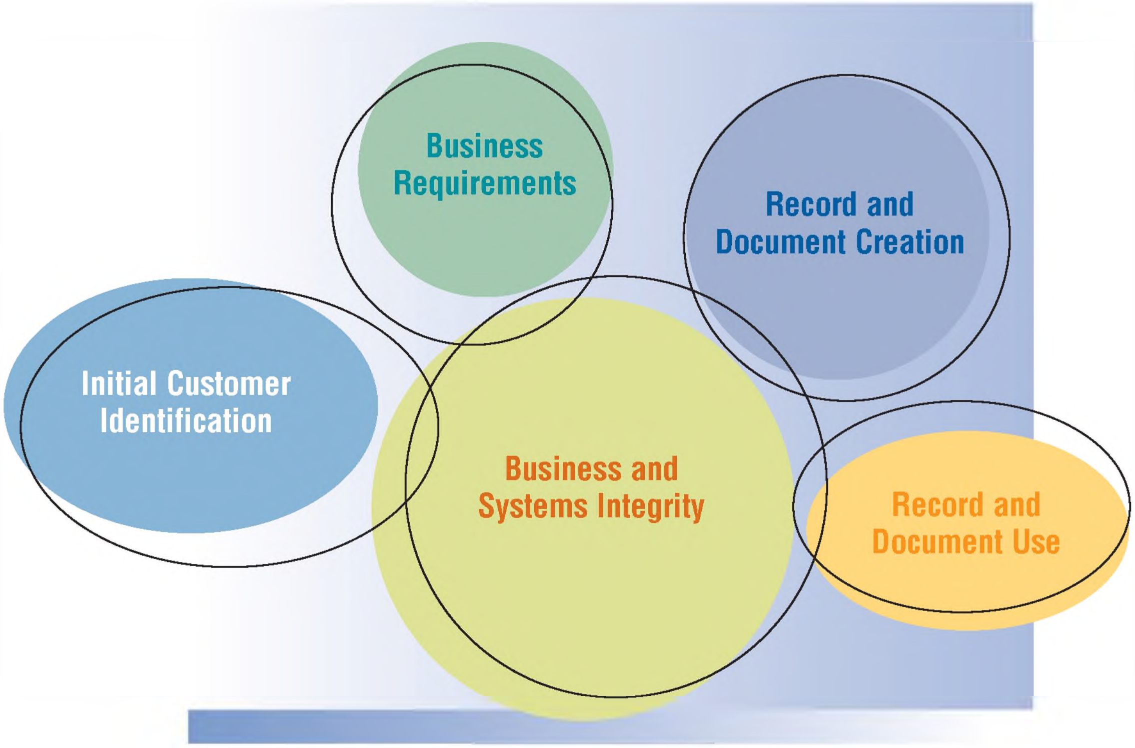
To satisfy this *Security Framework*, each Motor Vehicle Administration (MVA) must meet requirements and recommendations as given in shadow text throughout the document.

### Example:

**Requirement:** Each MVA shall... Requirements are mandatory obligations that the MVA must meet to satisfy this *Security Framework.*

**Recommendation:** Each MVA should... Recommendations are suggestions only. While optional, AAMVA advises that each MVA adopt the recommendations in this *Security Framework* as best practices.

The requirements and recommendations contained in this *Security Framework* are summarized as follows:


Business Requirements
Record and Document Creation
Initial Customer Identification
Business and Systems Integrity
Record and Document Use

## 1.1 Overview: Business Requirements

**Requirement #1:** Each MVA shall use the "*AAMVA Fraudulent Document Recognition (FDR) Model Training Program*" *(FDR Training Program)* in employee training programs for document fraud. The program addresses paper, laminated and plastic government identification documents.

**Requirement #2:** Each MVA shall conduct an internal review of document issuing systems, both manual and automated.

**Requirement #3:** All jurisdictions shall have at least one control measure in place for each risk area in their business process (see Appendix "03-4.2-03 Driver Licensing and Identification Business Processes—Risk Areas and Control Assessment" for a list of risk areas).

**Requirement #4:** All North American MVAs shall accept and endorse the eight privacy principles as specified in Appendix "05-4.5-03 Privacy Principles."

**Recommendation #1:** Each MVA should create a Risk Assessment Plan for those document issuing systems and then implement appropriate document fraud prevention and detection systems, as given in the white paper, to minimize both employee and customer fraud.

**Recommendation #2:** All MVAs should capture all procedures and business processes in writing.

**Recommendation #3:** All jurisdictions should become members of the Driver License Agreement (DLA), which has been enhanced to include the driver's license/identification card security requirements provided in this *Security Framework.*

## 1.2 Overview: Business and Systems Integrity

**Requirement #5:** All jurisdictions shall have an audit plan for their driver's license/identification card issuing processes (see Appendix "06-5.1-03 Framework for Audit Plan").

**Recommendation #4:** All jurisdictions should participate in a future compliance/oversight system to ensure the integrity of the minimum requirements for the secure issuance of a driver's license/identification card.

## 1.3 Overview: Initial Customer Identification

**Requirement #6:** All jurisdictions shall comply with the following definition of residency:

> *A person may only apply for and hold at any one time a driver's license from one jurisdiction. A person should be licensed in the jurisdiction where he/she spends the most time. In the event an individual divides his/her time in more than one jurisdiction, then the person must choose one jurisdiction in applying for and obtaining a driver's license.*
>
> *No person may be licensed by more than one jurisdiction at any one time. A jurisdiction shall not issue a driver's license to any individual who is licensed in another jurisdiction unless that individual is terminating licensure in the other jurisdiction.*

**Requirement #7:** Jurisdictions shall also use a verification process for ensuring that new applicants do not hold a driver's license from another jurisdiction, using the above definition of residency (AAMVA to develop verification guidelines).

**Requirement #9:** Wherever possible, all jurisdictions shall electronically verify the data elements required for driver's license/identification card issuance with the originator of those data elements.

**Requirement #8:**

- All U.S. jurisdictions shall use the Acceptable Verifiable Resource List for the United States and follow all associated procedures (see Appendix "07-6.2-03 U.S. Acceptable Verifiable Resource List").
- All Canadian jurisdictions shall use the Canadian Acceptable Verifiable List for Canada and follow all associated procedures (see Appendix "08-6.2-03 Canadian Acceptable Verifiable Resource List").

No foreign documents other than a passport shall be used (see Appendix "09-6.2-03 AAMVA Board of Directors Resolution 03-08: Use of Foreign Consular Cards for Identification Purposes").

## 1.4 Overview: Record and Document Creation

**Requirement #10:** All jurisdictions shall adhere to name collection, use and maintenance procedures as specified in Appendix “14-7.1-03 Name Collection, Use and Maintenance Procedures.”

**Requirement #11:** All jurisdictions that accept an immigration document as a source document shall tie the end-of-stay date to the expiration date of the driver’s license/identification card (see Appendix “15-7.2-03 End of Stay and DL/ID Expiration Procedures”).

**Requirement #12:** All jurisdictions shall follow the “Personal Identification—AAMVA International Specification—DL/ID Card Design” (AAMVA Card Specification) (see Appendix “17.7.3-03 Personal Identification—AAMVA International Specification —DL/ID Card Design”).

**Requirement #13:** The best unique personal identifier currently available is a framework of cross-verified data elements, especially the person’s name, date of birth and Social Security Number (U.S). These data elements must be collected as unique identifiers from the documents on the approved list of acceptable verifiable documents.

**Recommendation #5:** All jurisdictions should not grant a photo driver’s license/identification card to an undocumented immigrant (see Appendix “16-7.2-03 AAMVA Board of Directors Resolution 03-09: Position on Issuing Driver’s Licenses to Undocumented Aliens”).

## 1.5 Overview: Record and Document Use

**Recommendation #6:** All jurisdictions should have minimum penalties and sanctions for the unlawful use of a driver’s license/ identification card. Recommended minimum penalties and sanctions are listed in Appendix “25-8.1-03 Model Legislation: Minimum Penalties and Sanctions for Unlawful Application and/or Use of DL/ID Card.”

**Recommendation #7:** All jurisdictions should have legislation limiting the use of information collected and used from the machine-readable portion(s) of a driver’s license/identification card (see Appendix “26-8.2-03 Model Legislation: Limiting Information Collection and Use of Machine-Readable Technology”).

**Recommendation #8:** All jurisdictions should provide for data sharing between law enforcement and motor vehicle administrations including, but not limited to, exchanges of digital photos and driver records (see Appendix “27-8.3-03 White Paper on Data Sharing Between Law Enforcement and Motor Vehicle Administrations”).

# 2.0 Benefits

The recommendations and requirements presented in this document, once implemented, will provide each Motor Vehicle Administration (MVA) and other users of driver's license/identification cards (DL/ID) with the following benefits:

- A reduction in DL/ID fraud (resulting in improved road safety).
- A reduction in crime resulting from fraudulently obtained identification documents.
- Enhanced security and privacy of driver's license information within and between MVAs.
- Consistent minimum standards, policies and procedures among MVAs.
- A climate of innovation, encouraging both technological and procedural advances in driver licensing.

# 3.0 Introduction

## 3.1 Executive Summary

The driver's license is now the identification document of choice throughout North America. With a photo, signature, and physical description, the driver's license assumes a role beyond its original purpose of identifying a licensed driver. The license is now readily accepted as an official identification document for both licensed drivers, and, in most jurisdictions, for non-drivers. The Motor Vehicle Administrations (MVAs) who issue these documents have unique, continuous and long-lasting contact with most of their constituents from the individual's teenage years onward.

Most MVAs allow driver's license reciprocity with other MVAs; therefore a common security protocol among MVAs is necessary. This document provides minimum standards of security, interoperability and reciprocity agreed upon by all North American MVAs regarding driver's license/identification card (DL/ID) issuance. Each MVA shall:

- Either meet or exceed the requirements of the *Security Framework* based on risk analysis and resource availability.
- Determine that all individuals granted a DL/ID "are who they say they are."
- Ensure that each individual issued a DL/ID "remains the same person" throughout subsequent dealings both with itself or any other MVA.

Simply expressed, this means:

*one driver/identity—*
*one license document—*
*one driver control record*

throughout an individual's lifetime. Only a systematic and thorough approach ensures that minimum security standards and practices are met in each jurisdiction. Partial adherence may cause more harm than good, providing the appearance of security where in fact security does not exist.

A fraudulently obtained DL/ID leads to:

- Loss of life (e.g., unsafe drivers driving while suspended).
- ID-related fraud (e.g., credit card fraud, ID theft, passing bad checks, illegal purchase of alcohol).
- Fraudulently obtained entitlement to services or jobs (e.g., welfare fraud).
- Other criminal activity leading to economic and social losses.

This *Security Framework* provides requirements and recommendations for DL/ID issuance in the following areas:

- Business requirements (employee training, document issuing systems, internal controls and practices, the DLA and privacy)
- Business and systems integrity (audit plan, compliance and oversight)
- Initial customer identification (residency, resource lists and electronic verification)

- Record and document creation (name collection, use and maintenance, licensing noncitizens, card design specifications and unique identifiers)
- Record and document use (minimum penalties and sanctions, machine-readable technology legislation and data sharing)

## 3.2 Background

Over 10 years ago, AAMVA recognized a need to improve the inter-jurisdictional DL/ID issuance process. The implementation of the *U.S. Commercial Motor Vehicle Safety Act* of 1986 exposed security loopholes in the intra- and inter-jurisdictional driver's license processes. Individuals were readily able to obtain multiple driving privileges and identification either in their own or more than one jurisdiction.

AAMVA formed a Working Group that created the *1996 Uniform Identification Practices Model Program* to offer solutions to close some of the identification security loopholes. Components of the Program were adopted by several, but not all, MVAs, and no MVA adopted the Program in its entirety. In 2000, AAMVA created the Uniform Identification Subcommittee (UID Subcommittee), a permanent standing group reporting to the Driver License and Control Committee. The mandate of the UID Subcommittee was to reinstate and revise the work of the Uniform Identification Working Group.

After September 11, 2001, AAMVA established a Special Task Force on Identification Security. The Special Task Force made recommendations that the AAMVA Board of Directors accepted and turned over to the UID Subcommittee in January 2002. Throughout 2002 and 2003, the UID Subcommittee reviewed the DL/ID issuance practices of MVAs, law enforcement (LE) agencies and stakeholder communities. The Subcommittee also sought information and advice from the private sector, AAMVA members, the AAMVA Board of Directors and various consultants, federal agencies and associations (such as the IACP and NAPHSIS). Information was gathered via research, surveys, focus groups, expert advice, requests for information (RFIs), and requests for proposals (RFPs). The following *Security Framework* is the product of the recommendations resulting from that review.

## 3.3 Security Framework

Each MVA shall meet recommendations and minimum requirements in five areas to satisfy this *Security Framework*. The five areas are:

### 3.3.1 Business Requirements *(see Section 4.0)*

Identifies the policies and procedures as well as business systems and technology that an MVA shall have in place before it can issue a secure DL/ID. Components include:

- Employee training
  - Staff requirements
  - Fraud awareness and recognition
  - Exception handling
- Documentation
- Document issuing systems
  - Manual and automated systems necessary to support policies and procedures
- Internal controls and practices
  - Minimizing risk exposure
  - Staff awareness
  - Appropriate controls and protections
- The Driver License Agreement (DLA)
- Privacy

### 3.3.2 Business and Systems Integrity
*(see Section 5.0)*

Identifies the rules and practices of established business requirements. Components include:

- Audit plan
  - Specific plan for conducting an annual audit, including resource allocation
- Compliance and oversight

### 3.3.3 Initial Customer Identification
*(see Section 6.0)*

Provides procedures for positively identifying a customer and validating the customer's information. Components include:

- Residency
  - Customer obligations
  - Customer awareness
- Acceptable Verifiable Resource Lists and Procedures
- Electronic verification

### 3.3.4 Record and Document Creation
*(see Section 7.0)*

Provides procedures and specifications for creating a driver record and producing a DL/ID. Components include:

- Name collection, use and maintenance
- Licensing noncitizens
  - Expiration date
- Card design specifications
- Unique identifiers
  - Biometric and non-biometric

### 3.3.5 Record and Document Use
*(see section 8.0)*

Covers all legislation, policies and procedures associated with record and document use. Components include:

- Minimum penalties and sanctions
  - Enforcement of use of records and documents
  - Penalties and sanctions for unlawful application for and/or use of DL/ID
- Machine-Readable Technology (MRT) Legislation
  - Restrictions on use/collection of information
- Data sharing
  - Sharing of information between LE and MVAs

# 4.0 Business Requirements

Identifies the policies and procedures as well as business systems and technology that an Motor Vehicle Administration (MVA) shall have in place (requirement), or should have in place (recommendation), before it can issue a secure driver's license/identification card (DL/ID).

## 4.1 Employee Training

**Requirement #1:** Each MVA shall use the "*AAMVA Fraudulent Document Recognition (FDR) Model Training Program*" *(FDR Training Program)* in employee training programs for document fraud. The program addresses paper, laminated and plastic government identification documents.

The *FDR Training Program* provides standardized training material and training methods for all North American MVAs and law enforcement (LE) organizations in the following areas:

- Manual document review
- Fraudulent document recognition
- Customer service
- Interview techniques
- Fraud intervention
- Document examiner ethics

The *FDR Training Program* was developed by a working group of MVA and LE identification training experts then validated for content by the U.S. Secret Service and the Royal Canadian Mounted Police, in consultation with an independent training consultant for format and delivery. The Program ensures that training is comprehensive, consistent, and comprised of:

- *Instructor's Guide,* which provides unit lesson plans and instructor's visuals for teaching core subject matter. Lesson plans include content outlines, objectives, topics, teaching points, student activities, quizzes, end-of-course evaluation and visuals.
- *Level I Training* is designed as both initial and refresher training for MVA and LE staff and delivers a four-step fraud detection model evaluation process. Lesson plans include visual and tactile review of documents, interview techniques and document and document holder verification. The training is premised on the ability to evaluate and authenticate documents in a short time period. *Length: 12 hours.*
- *Level II Training* is designed as advanced training for supervisors, expert document examiners and fraud investigators and Level I is a prerequisite. Lesson plans include mid- to high-level security features and tools such as ultraviolet light and magnification techniques. The training is premised on a longer time period to more thoroughly evaluate and authenticate documents referred by Level I Examiners. *Length: 12 hours.*
- *FDR Instructor Preparation Workshop* is designed to teach trainers how to establish or enhance an MVA's fraud recognition training program. Lesson plans include teaching assignments and an end-of-course knowledge and practical evaluation with

an accumulative score of 80 percent or greater needed to receive a certificate of completion. *Length: 40 hours.*

See Appendix "01-4.1-03 FDR Training Program and Materials" for additional information on the content and use of the *FDR Training Program.*

### Benefits

The benefits of each MVA using the *FDR Training Program* in employee training programs for document fraud are:

- Consistency in training both within and across jurisdictions.
- A minimum level of knowledge and initial training on fraudulent document recognition for all employees
- Accelerated detection of fraudulent documents.
- Reduction in the acceptance of fraudulent documents.
- Increased public awareness of the fraudulent document security program.
- Heightened integrity of both the document and the associated motor vehicle record.
- Increased identification reciprocity among jurisdictions.
- Increased customer service.

## 4.2 Issuing Systems

**Requirement #2:** Each MVA shall conduct an internal review of document issuing systems, both manual and automated.

**Recommendation #1:** Each MVA should create a Risk Assessment Plan for those document issuing systems and then implement appropriate document fraud prevention and detection systems, as given in the white paper, to minimize both employee and customer fraud.

A white paper is provided that discusses both common and unique security techniques needed in over-the-counter, central and hybrid card issuing systems. After the mandatory internal review of document issuing systems, each MVA should implement the appropriate security measures as given in the white paper. Topics in the white paper are:

- Physical locations and security risk.
- Security risks in the supply chain.
- Securing card components.
- Security of personal information.
- Security risks of application processing.
- Risk assessment and developing a risk assessment plan.
- Staff monitoring.
- Quality control.
- Technology and associated security risks.

See Appendices "02-4.2-03 White Paper on Issuing Systems" and "03-4.2-03 Driver Licensing and Identification Business Processes—Risk Areas and Control Assessment"

### Benefits

The benefits of each MVA conducting an internal review of document issuing systems, creating a risk assessment plan, and implementing the appropriate security measures as given in the white paper are:

- Reduced employee and customer fraud.
- Enhanced fraud detection.
- Increased confidence by MVAs, LE agencies and the public in issued documents.
- Secure, common document issuing practices.
- Reduced identification theft.
- Privacy protection for personal information.

## 4.3 Documentation

**Recommendation #2:** All MVAs should capture all procedures and business processes in writing.

### Benefits:

The benefits of MVAs documenting all procedures and business processes are:

- Increased consistency of business processes (all staff perform the same procedure for a given business transaction).
- Reduced need for staff training.
- Increased reciprocity as procedures may be compared against those of other MVAs.
- Improved continuity of business processes (i.e., business process continue unchanged through staffing changes).

## 4.4 Internal Controls

**Requirement #3:** All jurisdictions shall have at least one control measure in place for each risk area in their business process (see Appendix "03-4.2-03 Driver Licensing and Identification Business Processes—Risk Areas and Control Assessment" for a list of risk areas).

In reviewing internal controls MVAs must also look at risk. Identifying and managing risk means establishing controls to limit the potential for fraud, therefore the two are in a cause-and-effect relationship.

There are many definitions for internal controls within the audit field. In this *Security Framework,* internal controls are:

*Mechanisms within the enterprise that have been designed to provide reasonable assurance regarding the achievement of the following objectives:*

- *Effective and efficient operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*
- *Safe and uniform application of the controls*

Further defined, internal controls are good operating practices that ensure an organization achieves its desired objectives. These controls provide assurance that information and data are recorded and reported as required. Internal controls are not a complete solution to an organization fulfilling its objectives but are instead an aid to achieving those objectives, to be used with other management practices.

In Ernst and Young's recent *8th Global Survey–Fraud-The Unmanaged Risk,* 85 percent of the worst frauds have been committed by insiders on the payroll of an organization.

Another trend evident in the survey was that more organizations are now establishing formal fraud prevention policies. To quote from the survey, *"Internal controls, management review and internal audit remain the most useful fraud prevention and detection factors."*

The internal control challenges faced by MVAs are similar to the challenges faced by any organization with a large number of employees conducting a variety of complex business processes in a decentralized manner. Some of the approaches to mitigating risk within any large organization are directly applicable to DL/ID processes. The cross-applicability of internal control challenges are summarized in Appendix "04-4.3-03 Internal Controls Best Practices" in the following four categories:

- Human Resources
- Auditing
- Information Technology
- Business Process

### Benefits

The benefits of all jurisdictions having at least one control measure in place for each risk area are:

- Appropriate checks and balances for all business processes, ensuring effective, consistent and efficient operations.
- Increased reliability of financial reporting.
- Ensured compliance with applicable laws and regulations.
- Safe and uniform application of procedures.
- Increased fraud deterrence and prevention.

## 4.5 Driver License Agreement (DLA)

**Recommendation #3:** All jurisdictions should become members of the Driver License Agreement (DLA), which has been enhanced to include the driver's license/identification card security requirements provided in this *Security Framework*.

The DLA is a voluntary, reciprocal agreement among member jurisdictions to promote the "one driver/identity—one license document —one driver control record" concept and to provide for the fair and impartial treatment of all drivers operating within its borders.

The DLA provides requirements for:

- Issuance and retention of DL/IDs.
- Establishing standards and procedures for DL/ID issuance.
- Updating and maintenance of driver records.
- Exchange of information between member jurisdictions.
- Compliance with the laws and regulations relating to highway safety and federal mandates.

Additionally, the DLA ensures uniformity and cooperation among MVAs in:

- Performing DL/ID procedures.
- Maintaining and sharing driver records.
- Protecting against identity fraud.
- Promoting reciprocity in the treatment of non-resident violators.

### Benefits

The benefits of all North American jurisdictions becoming members of the DLA are:

- Reduced DL/ID fraud.
- Increased jurisdictional cooperation and easier reciprocity.
- Ease for customers to clear issues in other jurisdictions.
- More efficient enforcement.

- Consistency and accuracy of driver's license information across jurisdictions.
- Potential for increased compliance with citations.
- Potential for increased collection of fines.
- Potential for reduction in license-related litigation.
- Improved driver's license record keeping.
- Cooperation among members to expedite problem resolution.

## 4.6 Privacy

**Requirement #4:** All North American MVAs shall accept and endorse the eight privacy principles as specified in Appendix "05-4.5-03 Privacy Principles."

To support AAMVA's efforts regarding the protection of personal information, the AAMVA Board of Directors issued a resolution determining that AAMVA will assist members with developing model contract provisions respecting access to personal information contained in motor vehicle records. In addition, the AAMVA Board of Directors supports the adoption of privacy principles and the implementation of best practices to ensure the protection and confidentiality of all personal information contained in the motor vehicle record.

Licensing information systems (both those currently in place and planned but not yet established) contain the personal information that is reasonable and necessary to accurately identify the individuals who hold DL/IDs. This information must be internally safeguarded, securely transmitted and properly interpreted. Decisions have been made and will continue to be made concerning the kinds of information that shall be kept and exchanged. While some of these issues involve technology, others involve policy. A foremost policy issue is the need to recognize and protect the privacy of individuals. Eight principles of privacy have been developed to address privacy issues in DL/ID issuance.

The eight privacy principles are:

1. **Openness:** Each MVA shall inform the public of all systems and databases that are being established or have been established for use in DL/ID 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 MVA and request the making of corrections to that data.

3. **Collection limitation:** Each MVA shall have a clear list of required personal data elements.

4. **Data quality:** Each MVA shall ensure that all data is "accurate, complete, current and verified."

5. **Use limitation:** Each MVA shall specify how it uses personal information and shall adhere to this specification.

6. **Disclosure limitation:** Each MVA shall adhere to a specified disclosure limitation that indicates what personal information may be disclosed and how it may be disclosed.

7. **Security.** Each MVA should protect all data kept.

8. **Accountability.** Each MVA shall ensure it has a means to oversee and enforce the previously mentioned principles.

### Benefits

The benefits of all MVAs adopting the eight principles of privacy are:

- Protection and confidentiality of all personal information obtained, stored and exchanged.
- Full compliance by all U.S. member jurisdictions with the terms of the federal Driver Privacy Protection Act[1], and full compliance by Canadian members with comparable national and provincial legal requirements.
- Informing the public of their rights and responsibilities regarding privacy.

[1] Title 18, Sections 2721, et seq. of the United States Code, hereinafter referred to as the DPPA *(Driver Privacy Protection Act).*

# 5.0 Business and Systems Integrity

Contains rules and practices ensuring Motor Vehicle Administrations (MVAs) comply with established audit and compliance requirements.

## 5.1 Audit Plan

**Requirement #5:** All jurisdictions shall have an audit plan for their driver's license/identification card issuing processes (see Appendix "06-5.1-03 Framework for Audit Plan").

Auditing may well be the most important aspect of internal control, and effective auditing is multi-layered. A formal, multi-layered audit plan is both an investigative control measure and a proactive deterrent to internal fraud.

An auditor must never have a role in the process that they are auditing; without this objectivity the audit process would be suspect.

### Benefits

The benefits of all MVAs having an audit plan are:

- Increased effectiveness and efficiency of operations.
- Increased reliability of financial reporting.
- Ensured compliance with applicable laws and regulations.
- Secure and uniform application of business practices.

## 5.2 Compliance and Oversight

**Recommendation #4:** All jurisdictions should participate in a future compliance/oversight system to ensure the integrity of the minimum requirements for the secure issuance of a driver's license/identification card.

The creation of a standardized quality assurance process is an integral component of a standardized driver's license/identification card (DL/ID) issuance process. Review of jurisdictional quality assurance practices and establishing minimum quality assurance standards ensures continuing reciprocity between jurisdictions.

There are currently several compliance and oversight systems in place in which AAMVA's membership is involved, such as the IRP peer review and the FMCSA CDL compliance review. The mechanism for compliance and oversight for the DL/ID security elements have been incorporated into the Driver License Agreement (DLA).

### Benefits

The benefits of all MVAs participating in a future compliance/oversight system are:

- Consistency of minimum standards.
- Continuing reciprocity among jurisdictions.

# 6.0 Initial Customer Identification

Provides requirements and recommendations for identifying a customer and validating the information presented by the customer. The section also identifies the rights and responsibilities of the customer concerning the personal information provided and how this information must be communicated to the customer.

## 6.1 Residency

**Requirement #6:** All jurisdictions shall comply with the following definition of residency:

*A person may only apply for and hold at any one time a driver's license from one jurisdiction. A person should be licensed in the jurisdiction where he/she spends the most time. In the event an individual divides his/her time in more than one jurisdiction, then the person must choose one jurisdiction in applying for and obtaining a driver's license.*

*No person may be licensed by more than one jurisdiction at any one time. A jurisdiction shall not issue a driver's license to any individual who is licensed in another jurisdiction unless that individual is terminating licensure in the other jurisdiction.*

**Requirement #7:** Jurisdictions shall also use a verification process for ensuring that new applicants do not hold a driver's license from another jurisdiction, using the above definition of residency (AAMVA to develop verification guidelines).

This definition of residency allows all jurisdictions to identify and coordinate issues regarding residency and determine an individual's jurisdiction of record. (The DLA provides a definition of residency that will supersede this definition once signed by all jurisdictions.)

The jurisdiction of record will control the activities of the individual's record for identification and highway safety purposes, further supporting the concept of "*one driver/identity—one license document—one driver control record.*" No matter where the record is kept, by design it will be the only record on the file system for the individual.

Note: The definition of residency does not address the **issue of legal presence** (whether a document *should* be issued), but merely helps determine which jurisdiction is responsible for issuing the individual's license and creating and maintaining the individual's driver record.

Exception: **Foreign Missions:** In the U.S., the Department of State through its Diplomatic Motor Vehicle Office has the sole authority to issue driver's licenses and motor vehicle registrations/titles for foreign missions and foreign mission members. No foreign mission or mission member may legally apply for or receive, and no state may issue a state driver's license, or motor vehicle title, registration and license plates in contravention of the limitations and conditions imposed by the Department of State.

### Benefits

The benefits of all MVAs using a common working definition of residency are:

- Assurance that each driver resides in a particular jurisdiction at a particular address.
- Customized driver programs based on the jurisdiction in which the driver lives.
- Awareness of the jurisdictional legal requirements, which apply to the driver, by both the driver and the MVA.
- Revenue is collected appropriately by jurisdiction.
- Drivers are licensed in the jurisdiction in which they live (not in another jurisdiction with less restrictive requirements).
- A continued definition and framework of "jurisdiction" until the DLA, along with associated communication and verification programs, is widely implemented.
- Consistent laws defining residency for all jurisdictions.
- Clearly defined requirements for license exchange.
- Elimination of out-of-jurisdiction driver's license.

## 6.2 Resource Lists and Procedures

**Requirement #8:**

- All U.S. jurisdictions shall use the Acceptable Verifiable Resource List for the United States and follow all associated procedures (see Appendix "07-6.2-03 U.S. Acceptable Verifiable Resource List").
- All Canadian jurisdictions shall use the Canadian Acceptable Verifiable List for Canada and follow all associated procedures (see Appendix "08-6.2-03 Canadian Acceptable Verifiable Resource List").

No foreign documents other than a passport shall be used (see Appendix "09-6.2-03 AAMVA Board of Directors Resolution 03-08: Use of Foreign Consular Cards for Identification Purposes").

To issue a secure driver's license/identification card (DL/ID), the source documents used to issue the card must be reliable and verifiable. Rather than requiring specific documents, the new Resource List protocol uses specific data elements found on the source documents to determine a customer's identity. To authenticate the new Resource Lists, the issuing agencies were asked how the source documents were issued. The result is a substantially reduced list of acceptable resources compared to the list found in the *AAMVA 1996 Uniform Identification Practices Model Program.*

Administrative procedures and exception processes also have been developed to assist jurisdictions in using the acceptable resource lists. To maintain the authenticity and reliability of the lists, a process has been developed to routinely review available resources and add/delete documents as needed.

### Benefits

Benefits of both Canada and the United States using the Acceptable Verifiable Resource Lists are:

- Minimum identification standards for all jurisdictions.
- Elimination of inconsistencies between jurisdictions, as all jurisdictions use the same data elements on supporting documentation rather than specified documents.
- Enhanced identification reciprocity between jurisdictions based on the use of the same verified data elements.
- Streamlined procedures for frontline staff.
- A fair and equitable DL/ID issuance process for all individuals.
- A uniform, verifiable and accurate DL/ID issuance process across all jurisdictions.
- Simplified and clarified exception handling.
- Protected personal customer information (the resources identified are verifiable).
- Accurate information from the DL/ID for LE.
- Consistent inclusion of all name information associated with the customer on the DL/ID, including the full legal name.
- Reduction in the number of documents required for identification due to the quality and reliability of the documents listed.
- No requirements for applicants to present additional identification resources when applying for a DL/ID.

## 6.3 Electronic Verification

**Requirement #9:** Wherever possible, all jurisdictions shall electronically verify the data elements required for driver's license/identification card issuance with the originator of those data elements.

Standardizing DL/ID issuing requires both close manual examination of hard copy documents and electronic verification of that document by the issuing agency. The issuing agency shall verify document:

- Issuance.
- Validity.
- Completeness (the document contains the required data elements).

Whenever possible, the information on the documents should be verified directly with the source document issuing agency (e.g., Social Security Numbers should verified with the Social Security Administration [see Appendix "10-6.3-03 Social Security Number Verification Best Practices"], immigration documents should be verified with the U.S. Bureau of Citizenship and Immigration Services). Other data elements, such as an address, should be verified with the U.S. Postal Service or through a third-party vendor (see Appendices "11-6.3-03 Address Verification Best Practices" and "12-6.3-03 Third Party Services for Verification Best Practices").

A verification matrix is provided to assist jurisdictions with a uniform method to verify each document on the Acceptable Verifiable Identification Resource Lists (see Appendix "13-6.3-03 Verification Matrix").

Several pilot projects are underway to determine if other methods of electronic data verification are viable.

- **Online Verification of Driver's License/ Identification Cards Pilot.** Examines electronic data verification of DL/IDs between MVAs and others public and private sector entities.

- **Digital Image Access Pilot.** Examines electronic data verification of digital images between jurisdictions.

- **Electronic Verification of Vital Events Records Pilot.** Examines electronic data verification of vital events records between MVAs and bureaus of vital statistics.

- **Implementation of the Ability to Perform Status and History Checks of All Drivers.** Examines electronic data verification of status and history checks between MVAs.

Each of these pilot projects will enhance the electronic verification process if successful and fully implemented.

### Benefits

The benefits of all MVAs electronically verifying, wherever possible, the data elements required for DL/ID issuance with the originator of those data elements are:

- Increased reciprocity between MVAs because of consistent and accurate electronic data verification.
- Reduction in attempts by customers to use fraudulent documents.
- Reduction in the acceptance of fraudulent documents.
- Enhanced database integrity.
- Increased accuracy in identifying individuals by LE.
- Easier and more consistent DL/ID application process for frontline employees.
- Reduction in confrontational incidents between customers and employees.
- Increased confidence from MVAs (and other stakeholders/organizations) in data sharing.

# 7.0 Record and Document Creation

Identifies procedures and specifications for creating records and producing a driver's license/identification card (DL/ID).

## 7.1 Name Collection, Use and Maintenance

**Requirement #10:** All jurisdictions shall adhere to name collection, use and maintenance procedures as specified in Appendix "14-7.1-03 Name Collection, Use and Maintenance Procedures."

The name is a critical data element used by jurisdictions to collect, record, store, display and match identification data. To ensure uniformity and accuracy, the complete name shall be collected upon initial application. An accurate driver record and a "day forward record keeping system," where accuracy is guaranteed from the inception date forward, can then be developed.

The full name breaks down into three segments.

1. Family name—last name(s).
2. Given name—first name(s) and middle name(s).
3. Suffix.

Collecting as much of an individual's name as possible to form the base name record will make accurate identification more likely.

Collecting and linking all name variations is necessary to prevent multiple DL/IDs since various events may affect the base name record (e.g., adoption, marriage, divorce, court orders).

Processing guidelines for name collection, use and maintenance are attached as Appendix "14-7.1-03 Name Collection, Use and Maintenance Procedures."

### Benefits

The benefits of all jurisdictions adhering to the procedures in Appendix "14-7.1-03 Name Collection, Use and Maintenance Procedures" for collecting, recording, storing, displaying and matching an individual's name are:

- Minimum standards for the collection, use, maintenance and storage of an individual's name in all jurisdictions.
- Increased reciprocity from more accurate matching of driver records using the individual's name as a key data element.
- Better customer service by MVAs when transferring a DL/ID, as driver records can be matched more accurately and efficiently.
- Increased protection of a customer's personal information and minimized identity theft, as legal name appears on the DL/ID and changes to the legal name appear on the driver record.
- Reduction in identification errors (e.g., citation convictions being updated to the wrong record) due to the use of full legal name.
- Reduction in erroneous hits on name searches because complete customer personal information is on file.

- Consistent name format (all staff, all jurisdictions use same format to enter and retrieve an individual's name).
- Reduction in manual processing and more automated search and matching decisions.
- Reduction in exception handling, and where necessary, simplified and clarified.

## 7.2 Licensing Noncitizens

**Requirement #11:** All jurisdictions that accept an immigration document as a source document shall tie the end-of-stay date to the expiration date of the driver's license/identification card (see Appendix "15-7.2-03 End of Stay and DL/ID Expiration Procedures").

**Recommendation #5:** All jurisdictions should not grant a photo driver's license/identification card to an undocumented immigrant (see Appendix "16-7.2-03 AAMVA Board of Directors Resolution 03-09: Position on Issuing Driver's Licenses to Undocumented Aliens").

The number of noncitizens (both legal and illegal) applying for a DL/ID has steadily increased in recent years. A documented immigrant may have one of several status classifications, which may cause confusion when he/she applies for a DL/ID. Immigration status and an immigrant's length-of-stay in the country have been identified as factors in national security. DL/ID issuance of immigrants must therefore be a consistent, accurate and secure process.

Noncitizens may be separated into two groups for the purposes of DL/ID issuance:

1. Documented immigrants with temporary status
2. Undocumented immigrants

Each group is discussed separately below in sections 7.2.1 and 7.2.2.

### 7.2.1 Documented Immigrants

Expiring the DL/ID on the end-of-stay (end of the visa) date requires:

- Original or certified immigration documents upon application.
- Issuance of the DL/ID with an expiration date that matches the lawful presence expiration date (end-of-stay date) or the jurisdiction's standard renewal cycle expiration date, whichever is shorter.
- Defined procedures for cases that require exception processing and management approval.

Detailed procedures for implementing the process are found in Appendix "15-7.2-03 End of Stay and DL/ID Expiration Procedures."

#### Benefits

The benefits of expiring the DL/ID on the end-of-stay date are:

- DL/ID issuance motivates customers to keep status valid with Bureau of Citizenship and Immigration Services (BCIS).
- Standardized procedures for reciprocity when immigration status is authorized by BCIS.
- Easier enforcement of laws regarding end-of-stay date/card expiration date.
- Elimination of calculation errors as end-of-stay date is provided by BCIS.
- Increased control, as DL/ID issuance is eliminated without appropriate BCIS documentation.

### 7.2.2 Undocumented Immigrants

In May 2003, AAMVA recommended that jurisdictions not grant a photo DL/ID to an undocumented immigrant. To strengthen the security of the photo DL/ID and the issuance process associated with it, it is necessary to increase the standards for an individual proving his/her identity to obtain a license.

Increasing standards for all individuals strengthens uniformity, encourages reciprocity in motor vehicle administration and enhances highway safety enforcement. The official text of the AAMVA Board of Directors Resolution is found in Appendix "16-7.2-03 AAMVA Board of Directors Resolution 03-09: Position on Issuing Driver's Licenses to Undocumented Aliens."

## 7.3 Card Design Specifications

**Requirement #12:** All jurisdictions shall follow the "Personal Identification—AAMVA International Specification—DL/ID Card Design" (AAMVA Card Specification) (see Appendix "17.7.3-03 Personal Identification—AAMVA International Specification—DL/ID Card Design").

One of the most important components of any personal identification system is the finished card issued to the individual. 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. As such, cards must be readily recognizable as genuine and need to be protected against fraud.

The goals of the AAMVA Card Specification are functionality, interoperability, compatibility, commonality and security.

The five functions of a DL/ID are:

1. Evidence of privilege to drive.
2. Identification.
3. Age verification.
4. Address/residence verification.
5. Automated administrative processing.

The DL/ID must be compatible with those of other jurisdictions because of the highly mobile population in North America, often appearing in jurisdictions other than where the DL/ID was issued. Law enforcement (LE), Motor Vehicle Administrations (MVAs) and other stakeholders and users must be able to authenticate and collect information from DL/IDs issued in their own and other jurisdictions.

Commonality in card design is necessary to simplify comparison of data elements and enhance reciprocity. There are hundreds of card variations across North America, which creates confusion, hampers recognition and authentication of genuine documents, and prevents detection of fraudulent DL/IDs by LE and other users.

The AAMVA Card Specification describes a common design and physical layout for DL/IDs where each data element is prescribed a zone on both the front and back of the card. Data elements appear on the card in both human and machine-readable formats.

Some common design features prescribed by the AAMVA Card Specification are:

- PDF417 2-dimensional barcode required as the common machine-readable technology.
- Horizontal vs. vertical format specified as:
  - Horizontal format (age 21 and over).
  - Vertical format (under age 21).
- Portrait location on the left side.
- Data elements defined, such as document discriminator, audit information number, customer identification number, inventory control number, use of full name, physical characteristic descriptions.
- Data elements specified as either mandatory or optional.
- Where possible, specifications compatible with work done by International Organization for Standards (ISO) on developing an international standard for the driver's license.

Establishing a common security baseline for documents among jurisdictions is necessary; as currently each jurisdiction uses different security measures for card issuance. Some cards exhibit many security features while others contain little protection for security risks and threats. While no one security plan meets all needs, several proven techniques meet specific security requirements.

To provide a common security protocol for all jurisdictions, the AAMVA Card Specification provides minimum card security specifications in the following threat areas:

- Counterfeit/simulation
- Alteration/forgery
- Cannibalization (using parts of cards together)
- Photo/signature substitution

Approved security techniques and devices are specified and criteria provided so that all jurisdictions may use these techniques to provide a common, minimum level of security. The AAMVA Card Specification provides criteria to use the security techniques in a layered and structured application and at all three levels of security (first, second and third line inspection). Levels of security are defined as:

- **Level 1,** first line—inspection visible to the human eye or apparent to touch.

- **Level 2,** second line—inspection requiring the use of a tool or instrument (e.g., magnifying glass, UV light).

- **Level 3,** third line—inspection requiring higher level of exploration (e.g., microscope).

The AAMVA Card Specification provides criteria for the following security issues:

- Security Device Index
- Minimum acceptable level of security devices to cover all threat levels
- Level 1, 2, and 3 (first, second, and third line) inspection devices
- Mandatory level 1 security device (3-dimensional optical variable device)
- Common machine-readable technology (PDF417 2-dimensional barcode)

### Benefits

The benefits of all jurisdictions using the AAMVA Card Specification are:

- Reduced identification theft and fraud.
- Increased card security.
- Improved uniformity of data elements.
- Easier authentication of genuine DL/IDs and better recognition of fraudulent documents.
- Increased confidence in DL/IDs by the LE community, other users and stakeholders.
- Continued and improved data exchange and reciprocity among jurisdictions.
- More ease and security in transfer of information.
- Uniform, machine-readable format for data elements, facilitating automation and reducing processing errors.
- Facilitation and expedition of initial card inspection by a casual and trained observed based on a common Level 1 security device.
- Facilitation of collection and authentication of card data in both human and machine-readable formats for LE and MVAs.
- Common, minimum security levels for all DL/IDs for all jurisdictions.

## 7.4 Unique Identifiers

**Requirement #13:** The best unique personal identifier currently available is a framework of cross-verified data elements, especially the person's name, date of birth and Social Security Number (U.S). These data elements must be collected as unique identifiers from the documents on the approved list of acceptable verifiable documents.

When an applicant enrolls for the first time, the MVA attempts to verify that the applicant is who he/she claims to be. The MVA manually inspects source documents and verifies electronically the authenticity and status of the documents with the originator (e.g., the Social Security Administration, Immigration Services). The MVA checks their own records, those of other MVAs, other systems (e.g., PDPS, IRE and CDLIS), and may use a third-party service to verify some or all of the information presented by the applicant to ensure that the individual is not already identified elsewhere and attempting to obtain multiple documents.

MVAs must know, on a continual basis, with whom they are conducting business. A proper unique identifier must be defined for each MVA business process (enrollment, verification and updating). A unique identifier can be either biometric (biological in origin such as fingerprints, voiceprints, iris and retina scans, hand measurements and signature dynamics) or non-biometric (combination of data such as full name, date of birth, demographics, physical characteristics and customer and document numbers). Biometric and non-biometric identifiers are discussed separately in sections 7.4.1 and 7.4.2.

### 7.4.1 Biometric Identifiers

The possibility of using physiological biometric identifiers to satisfy at least some of the requirements of a unique identifier has been considered. Ultimately, using biometric identifiers holds the promise of a real solution to the problems of identity theft and multiple identities by the same person.

However, for a biometric technology to be selected and to be interoperable in North America, it must perform a one-to-many (1–N) record matching or identification function. To date, there have not been any large scale uses of biometric technologies that have performed one to many record matching for populations the size MVAs need to address (300 million records). See Appendix "19-7.4-03 Final Report—Phase 1: Technical Capability of Biometric Systems to Perform 1:300m Identification. International Biometric Group."

The current methods of measuring biometric technologies are not adequate for the type of system that AAMVA proposes. The majority of the research, reports and findings for biometric technologies are related to systems that perform the one-to-one matching. AAMVA suggests that more information is needed to reach a decision. An "Information Needs" report is found as Appendix "21-7.4-03 Biometric Technology Information Needs (Fischer Consulting Inc.)."

Guidance to jurisdictions considering their own biometric technologies is offered in Appendix "22-7.4-03 Guidance to Jurisdictions Considering Biometric Technology in Interim." Each jurisdiction also will benefit from the overall work already documented in terms of the decision support criteria provided in the report attached as Appendix "20-7.4-03 Structured Decision Making Roadmap for the Evaluation of Biometric Technologies in a Driver's License Environment (Fischer Consulting Inc.)."

### 7.4.2 Non-Biometric Identifiers

For any activity on the driver record after initial enrollment (e.g., renewals, amendments, address changes), the MVA must be assured that it is dealing with the same verified person that was accepted for enrollment. At times, the individual may not be present as the driver record is updated (e.g., as enforcement activities progress through the justice system from citation to the conviction stage) and in these cases, the MVA relies heavily on information previously collected concerning the "uniqueness of the individual." This "unique identifier" is a combination of full name, date of birth, demographics, physical characteristics and customer and document numbers. This unique identifier ensures that the correct record is updated.

In the absence of a biometric identifier, more emphasis must be placed on the creation of non-biometric identifiers. Considerations for the secure collection and verification of traditional data elements for use as non-biometric identifiers are:

- Name: The individual's full name must be collected. If the entire name is not collected as a base record at the time of initial application, the information is lost and not useful in the future for any matching schemes.
- SSN: Collection and validation of the Social Security Number (SSN) in the United States is critical.
- DOB: Accurate, verified date of birth (DOB) differentiates individuals and the associated driver record from one another.
- Demographics and physical description information must be examined more critically and provided more accurately on the DL/ID.
- Several generated numbers are described in the AAMVA Card Specification that will link the customer and the DL/ID back to the automated record (e.g., customer identifier, document discriminator, audit number).
- A system to exchange digitized photos is being developed and piloted to facilitate accurate identification of individuals (see Appendix "24.7.4-03 Digital Image Exchange Pilot Project").
- The PDF417 2-dimensional bar code will aid in collecting and transmitting information with minimal transcription error.

The added security features of the DL/ID will protect the unique, non-biometric identifier from being counterfeited/simulated, altered or cannibalized, and from photo/signature substitution.

See Appendix "18-7.4-03 Business Requirements for the Unique Identifier." Business requirements for a unique identifier used in the MVA environment are addressed in Appendix "23-7.4-03 Technology Assessment Phase II: Assessment of Alternative Technologies and Unique Identifiers."

# 8.0 Record and Document Use

Provides policies and practices for the use of motor vehicle records and issued documents and minimum penalties and sanctions for their misuse.

## 8.1 Minimum Penalties and Sanctions

**Recommendation #6:** All jurisdictions should have minimum penalties and sanctions for the unlawful use of a driver's license/identification card. Recommended minimum penalties and sanctions are listed in Appendix "25-8.1-03 Model Legislation: Minimum Penalties and Sanctions for Unlawful Application and/or Use of DL/ID Card."

A strong incentive for compliance is necessary to ensure the integrity and security of any driver's license/identification card (DL/ID) issuing system and its legal requirements, rules and procedures. Penalties and sanctions must provide a sufficient deterrent so that individuals do not break the law. Without sufficient penalties and sanctions, the licensing system is flawed and vulnerable to fraudulent activities from both the outside and within.

It is therefore necessary to have, both on a jurisdictional and federal level, the proper minimum penalties and sanctions in place to deter unlawful use of the DL/ID. The U.S. Department of Justice and the U.S. Federal Trade Commission are working to introduce new legislation that increases federal penalties for identification theft.

At the jurisdictional level, Law Enforcement (LE) will be more likely to investigate and prosecute crimes of DL/ID fraud if these crimes have recommended minimum penalties and sanctions, and convictions are more likely.

### Benefits

The benefits of all jurisdictions having minimum penalties and sanctions for the unlawful use of a DL/ID are:

- Deterrence of individuals committing fraud.
- Reduced fraud and increased system integrity.
- Increased interest by LE and prosecutors to prosecute fraud cases.

## 8.2 Machine-Readable Technology Legislation

**Recommendation #7:** All jurisdictions should have legislation limiting the use of information collected and used from the machine-readable portion(s) of a driver's license/identification card (see Appendix "26-8.2-03 Model Legislation: Limiting Information Collection and Use of Machine-Readable Technology").

Jurisdictions have privacy concerns regarding the use and misuse of data encrypted on the DL/ID in the machine-readable format.

The AAMVA Card Specification requires that the PDF-417 2-dimensional bar code be used as the common machine-readable technology (MRT) on each DL/ID. Additional MRTs may be used in conjunction with the bar code. The AAMVA Card Specification furthermore states that any data item contained in the human-readable portion of the license should not be encrypted in the MRT.

Encryption either defeats or complicates the use of MRT. Currently, a number of jurisdictions are developing automated systems for generating and processing citations, crash reports and other similar documents. These automated systems incorporate MRT. If encrypted, the MRT data is not available to any LE activity that does not share the decryption key. The distribution and control of the decryption key therefore becomes the critical element, and the two keys must be controlled if access to the data is restricted.

The large number of potential key holders involved compounds the problem of key control. Some estimates place the number of LE agencies in the United States as high as 14,000. Each of these agencies must have all necessary decryption keys, and either the key is so widely distributed as to be insecure or a large number of legitimate users are unable to read the data.

### Benefits

The benefits of all jurisdictions having legislation limiting the use of information collected and used from the machine-readable portion(s) of a DL/ID are:

- Defined rules regarding the use of MRT data.
- A greater degree of control by the DL/ID holder over the card and the information contained on it.
- Improved reciprocity and interoperability based on non-encrypted common MRT, as defined by the legislation.

## 8.3 Data Sharing

**Recommendation #8:** All jurisdictions should provide for data sharing between law enforcement and motor vehicle administrations including, but not limited to, exchanges of digital photos and driver records (see Appendix "27-8.3-03 White Paper on Data Sharing Between Law Enforcement and Motor Vehicle Administrations").

There are many public safety reasons for MVAs to share, in real time, DL/ID data. Enhancements by individual MVAs are inadequate without provisions for data sharing with other MVAs. Data sharing is necessary to prevent individuals from fraudulently obtaining or falsifying the information on DL/IDs and for MVAs to adequately share information about unsafe drivers. This ensures only qualified applicants are licensed to drive and increases road safety.

The data shared may include a digital image.

Additionally, LE depends on the digital image and associated driver record to:

- Identify a criminal suspect.
- Accurately make decisions concerning driver record status at roadside.
- Ensure the highest degree of officer safety.
- Protect the public by identifying criminals.

As access to data increases, the possibility of both misuse and error increase. AAMVA must provide leadership and direction concerning the legitimate use of driver data, and must provide direction when error or misuse occurs. While the exchange of personal information can save lives, MVAs must ensure privacy and protection of all DL/ID data.

### Benefits

Real-time data sharing between jurisdictions, which may include the sharing of a digital image, has the following benefits:

- Keeps unsafe drivers from obtaining a license following suspension or revocation.
- LE can verify an individual's identity at roadside.
- LE can verify an individual's identity both preparing for and during an investigation.
- Identifies individuals who pose a potential national security threat.
- Verifies an individual's identity prior to a transaction.

# 9.0 Glossary of Abbreviations and Acronyms

The following is a glossary of abbreviations or acronyms that appear in this document:

- AAMVA: American Association of Motor Vehicle Administrators
- BCIS: Bureau of Citizenship and Immigration Services
- CCMTA: Canadian Council of Motor Transport Administrators
- CDL: Commercial Driver's License
- CDLIS: Commercial Driver's License Information System
- DLA: Driver License Agreement
- DL/ID: Driver's License/Identification Card
- DPPA: *Driver Privacy Protection Act* (U.S.)
- DRIVerS: an all-driver pointer system (Driver Record Information and Verification System)
- FDR Training Program: AAMVA Fraudulent Document Recognition Model Training Program
- FMCSA: Federal Motor Carrier Safety Administration
- IACP: International Association of Chiefs of Police
- LE: Law Enforcement
- MRT: Machine-Readable Technology
- MVA: Motor Vehicle Administration
- NAPHSIS: National Association of Public Health Statistics and Information Systems
- UID Subcommittee: Uniform Identification Subcommittee

# 10.0 Acknowledgements

The authors of this *Security Framework* offer a special thank you to the countless individuals and organizations whom provided their expertise and contributed to this effort. Many individuals have shown dedication to the effort through focus groups, responding to requests for information (RFIs) surveys and endless research.

The following experts, as members of the Uniform Identification Subcommittee and/or Task Groups, provided extensive input on AAMVA's efforts to improve identification security. The Association recognizes these individuals' efforts and appreciates the dedication and commitment each individual demonstrated toward enhancing identification security throughout North America.

### SPECIAL TASK FORCE ON IDENTIFICATION SECURITY

*Pennsylvania Department of Transportation*
Betty Serian, Chair

*Canadian Council of Motor Transport Administrators*
Audrey Henderson

*Indiana State Police*
Major John Hill

*New Jersey Department of Motor Vehicles*
W. Patrick Scheffer

*New York Department of Motor Vehicles*
Joe Sanders

*North Dakota Division of Motor Vehicles*
Keith Kiser

*Saskatchewan Government Insurance*
Alan Cockman

*Texas Department of Public Safety*
Michael Anderson

*Texas Vehicle Titles & Registration Division*
Jerry Dike

*AAMVA*
Linda R. Lewis
Michael R. Calvin
Jay Maxwell
Tom Wolfsohn

### MOTOR VEHICLE ADMINISTRATION

*Alabama Driver License Division*
Curtis Terling

*Arizona Motor Vehicle Division*
Craig Stender

*California Department of Motor Vehicles*
Marilyn Schaff
Michele Snyder
Jayme L. Hyde

*Delaware Division of Motor Vehicles*
Jerome Emerson

*Florida Department of Highway Safety & Motor Vehicles*
Mike Alderman

*Georgia Department of Motor Vehicle Safety*
Tim Burgess

*Illinois Office of the Secretary of State, Driver Services*
Lucy Kelly

*Iowa Motor Vehicle Division*
Terry Dillinger

*Kentucky Department of Vehicle Regulation*
Gary Brunker

*Massachusetts Department of Public Safety*
James Slater

*Montana Motor Vehicle Division*
Brenda Nordlund
Anita Drews-Oppedahl

*Missouri Department of Revenue*
Shelly Jackson

*Newfoundland and Labrador, Department of Government Services and Lands*
Carolyn Burggraaf

*New York Department of Motor Vehicles*
Joe Sanders (inaugural Uniform ID Subcommittee Chair)
Kevin O'Brien
Adam Gigandet

*North Carolina Division of Motor Vehicles*
Wayne Hurder

*Nova Scotia Registry of Motor Vehicles*
Donna Arseneau

*Ohio Bureau of Motor Vehicles*
Carolyn Williams

*Oklahoma Department of Public Safety*
Clint Dickson

*Colorado Motor Vehicle Business Group*
Debora Jerome

*Connecticut Department of Motor Vehicles*
John Yacavone
Barbara Tanuis

*Ontario Ministry of Transportation*
Vivienne Cameron
Ross Burns
Sarah Gale

*Pennsylvania Department of Transportation*
Steve Kozar

*Saskatchewan Driver & Vehicle Safety Services*
Bernadette McIntyre

*Saskatchewan Government Insurance*
Donnie Courchaine

*Société de l'assurance automobile du Québec*
Claude Gelinas

*Texas Department of Transportation*
Jack Durham

*Utah Department of Public Safety*
Skip Nielsen

*Virginia Department of Motor Vehicles*
Jo Anne Maxwel
Vicky Mercer

*West Virginia Department of Transportation*
Robert Mullins

*Wisconsin Division of Motor Vehicles*
Karen Schwartz

*Wyoming Department of Transportation*
Deb Ornelas

### LAW ENFORCEMENT

*Arizona Department of Transportation*
John Rodi

*Colorado Highway Patrol*
Col. Mark Trostel

*Florida Division of Alcoholic Beverages & Tobacco*
Maj. David Myers

*Florida Highway Patrol*
Chief John Czernis
Lt. Col. Billy Dickson

*Iowa Motor Vehicle Enforcement*
Kerry Kirkpatrick
Paul J. Steier

*Kansas Highway Patrol*
Col. Don Brownlee

*Maryland Department of Public Safety*
Tom Steele

*North Carolina State Highway Patrol*
Isaac T. Avery

## FEDERAL AGENCIES

*Department of State (DOS)*
Jacqueline Robinson

*Federal Motor Carrier Safety Administration (FMCSA)*
Bonnie Bass
Carol Gore
Robert Redmond

*National Highway Traffic Safety Administration (NHTSA)*
Sean McLaurin
Glenn Karr

*Transportation Security Administration (TSA)*
Dan Hartman (formerly FMCSA)
Larry Slade (formerly FMCSA)
Mary Ann McNamanra

*United States Secret Service (USSS)*
Susan L. Fortunato
Richard L. Outland

*Royal Canadian Mounted Police (RCMP)*
Robert Moyes
Errol Schell

## CANADIAN COUNCIL OF MOTOR TRANSPORT ADMINISTRATORS (CCMTA)

Audrey Henderson
Martin Jackson

## AAMVA STAFF

Linda Lewis
Michael R. Calvin
Rich Carter
Melissa Clague
Selden Fritschner
Randy Holleger
Harold Kocken
Kevin Lewis
Jay Maxwell
James Nance
Pamela Richardson
Brett Robinson
Nathan Root
Marshall Stewart
Tracy Taillon
Donna West
Tom Wolfsohn
Renee Dejewski

# 11.0 Appendices

XX-YY-ZZ

XX = Sequence number

Y.Y = chapter and section number

ZZ = Year (last 2 digits)

| | |
|---|---|
| 01-4.1-03 | FDR Training Program and Materials |
| 02-4.2-03 | White Paper on Issuing Systems (Over-the-Counter, Central and Hybrid) |
| 03-4.3-03 | Driver Licensing and Identification Business Processes—Risk Areas and Control Assessment |
| 04-4.3-03 | Internal Controls Best Practices |
| 04-4.5-03 | Privacy Principles |
| 06-5.1-03 | Framework for Audit Plan |
| 07-6.2-03 | U.S. Acceptable Verifiable Resource List |
| 08-6.2-03 | Canadian Acceptable Verifiable Resource List |
| 09-6.2-03 | AAMVA Board of Directors Resolution 03-08: Use of Foreign Consular Cards for Identification Purposes |
| 10-6.3-03 | Social Security Number Verification Best Practices |
| 11-6.3-03 | Address Verification Best Practices |
| 12-6.3-03 | Third Party Services for Verification Best Practices |
| 13-6.3-03 | Verification Matrix |
| 14-7.1-03 | Name Collection, Use and Maintenance Procedures |
| 15-7.2-03 | End of Stay and DL/ID Expiration Procedures |
| 16-7.2-03 | AAMVA Board of Directors Resolution 03-09: Position on Issuing Driver's Licenses to Undocumented Aliens |
| 17.7.3-03 | Personal Identification—AAMVA International Specification—DL/ID Card Design |
| 18-7.4-03 | Business Requirements for the Unique Identifier |
| 19-7.4-03 | Final Report—Phase 1: Technical Capability of Biometric Systems to Perform 1:300m Identification. International Biometric Group |
| 20-7.4-03 | Structured Decision Making Roadmap for the Evaluation of Biometric Technologies in a Driver's License Environment (Fischer Consulting Inc.) |
| 21-7.4-03 | Biometric Technology Information Needs (Fischer Consulting Inc.) |
| 22-7.4-03 | Guidance to Jurisdictions Considering Biometric Technology in Interim |

23-7.4-03 Technology Assessment Phase II: Assessment of Alternative Technologies and Unique Identifiers

24.7.4-03 Digital Image Exchange Pilot Project

25-8.1-03 Model Legislation: Minimum Penalties and Sanctions for Unlawful Application and/or Use of DL/ID Card

26-8.2-03 Model Legislation: Limiting Information Collection and Use of Machine-Readable Technology

27-8.3-03 White Paper on Data Sharing Between Law Enforcement and Motor Vehicle Administrations

AAMVA

**American Association of**
**Motor Vehicle Administrators**

4301 Wilson Blvd, Suite 400
Arlington, VA 22203
Phone: 703-522-4200
Fax: 703-522-1553
Web: www.aamva.org