AAMVA DL/ID Security Framework

Executive Summary

Survey of the States on Implementation of Driver's License and Identification Card Reform

A Report by:

The American Association of Motor Vehicle Administrators

and

The Driver License Compact and Nonresident Violators Compact

Prepared by:

The AAMVA DL&C Implementation and Maintenance Subcommittee

May 2005

American Association of
Motor Vehicle Administrators

TABLE OF CONTENTS

INTRODUCTION

The American Association of Motor Vehicle Administrators (AAMVA) accelerated their efforts in 2001, following the events of September 11, to reform driver's license (DL) and personal identification card (ID) issuance. In January 2002, AAMVA charged the development of these best practices to the Uniform Identification (UID) Subcommittee, a subcommittee of the AAMVA Driver Licensing and Control (DL&C) Committee.

The UID Subcommittee was initially formed in the early 1990s to develop recommendations on uniform identification practices. The UID Subcommittee released a revision of the recommendations in 1996 titled the "Uniform Identification Practices – Model Program."

AAMVA partnered with the Driver License Compact (DLC) and Nonresident Violators Compact (NRVC) Executive Board in August 2002 to incorporate security requirements into the new Driver License Agreement (DLA) creating a comprehensive DL/ID issuance system.

In February 2004, AAMVA released the "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." For a motor vehicle administration (MVA) to declare compliance with the standards, they must meet the 13 requirements and 8 recommendations prescribed to satisfy the *Security Framework*. In November 2004, the DLC/NRVC Compacts Executive Board announced to its membership that the enhanced DLA would be finalized in early 2005 pending a vote of acceptance by MVA administrators.

In November 2004, the U.S. Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The Act included provisions for driver's license and personal identification card issuance reform. The Act charged the Secretary of the Department of Transportation (DOT) to develop minimum requirements for DL/ID issuance through a negotiated rulemaking process.

To assist AAMVA and its membership in the rulemaking process, the AAMVA Board of Directors and the Compacts Executive Board reached out to the AAMVA Implementation and Maintenance (IM) Subcommittee, to develop and conduct a telephone survey to ascertain the current status of jurisdictions on their efforts to implement the measures of the *Security Framework*.

The IM Subcommittee conducted detailed telephone interviews with each U.S. jurisdiction from February 22 through March 25, 2005. The responses to the telephone surveys are detailed in this report.

The telephone surveys will assist the AAMVA Board of Directors and the Compacts Executive Board to develop uniform positions on DL/ID security issues as they relate to the negotiated rulemaking process and other proposed congressional legislation.

BLANK PAGE

HOW TO USE THIS REPORT

This report is divided into eight main sections. The first seven sections correspond to the seven minimum standards of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) (hereafter referred to as Act) on driver's license and personal identification card reform. Below is a brief description of each of the minimum standards in the Act and the *AAMVA DL/ID Security Framework* requirements and recommendations that correspond.

SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card. Requirement 8 – acceptable verifiable resource list of the *Security Framework*.

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card. Requirements 7 – verification process, 8 – acceptable verifiable resource list, and 9 – electronically verify date elements of the *Security Framework*.

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud. Requirements 1 – FDR training, 3 – control measures, 5 – audit plan, 7 – verification process, 8 – acceptable verifiable recourse list, 9 – electronically verify data elements, 10 – name collection and maintenance procedures, 11 – tying end of stay to expiration date of DL/ID, and 13 – cross reference data elements; and Recommendations 1 – risk assessment plan, 2 – capture all procedures and business processes in writing, and 3 – membership in the DLA of the *Security Framework*.

SECTION D: The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature. Requirements 8 – acceptable verifiable resource list, 10 – name collection use and maintenance procedures, 12 – AAMVA Card Design Specs, and 13 – cross reference data elements of the *Security Framework*.

SECTION E: The Act requires the development of standards for common machine-readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements. Requirement 12 – AAMVA Card Design Specifications; and Recommendation 7 – limit use of information on Machine-Readable Technologies (MRT) of the *Security Framework*.

SECTION F: The Act requires the development of security standards to ensure that driver's license or personal identification card are (i) resistant to tampering, alteration, or counterfeiting; (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier. Requirement 12 – AAMVA Card Design Specifications of the *Security Framework*.

SECTION G: The Act requires that a state confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised. The *Security Framework* does not address confiscation of DL/IDs.

SECTION H: Survey Summary

To locate information on a specific section of the Act; refer to the appropriate section A–G. To locate information specific to the AAMVA *Security Framework*, please refer to sections A–F, to determine which *Security Framework* elements are continued within the Act sections. Please note that *Security Framework* elements may appear in multiple sections of the Act.

Comments and questions concerning this report should be addressed to Harold Kocken of the AAMVA Programs Division. AAMVA will strive to keep the content of this report up-to-date. We urge states to continue to provide any new information when available.

Mr. Harold Kocken
Senior Director, Programs Division
4301 Wilson Blvd., Suite 400
Arlington, VA 22203
hkocken@aamva.org

This survey report was developed with funding and support from the Federal Motor Carrier Safety Administration (FMCSA).

ACRONYMS AND ABBREVIATIONS

AAMVA	American Association of Motor Vehicle Administrators
Act	Intelligence Reform and terrorism Prevention Act of 2004
AKA	Also Known As
BCIS	U.S. Bureau of Citizenship and Immigration Services
BMV	Bureau of Motor Vehicles
CDL	Commercial Driver's License
CDLIS	Commercial Driver's License Information System
CVP	Courtesy Verification Program
DEERS	Defense Enrollment Eligibility Reporting System
DHS	Department of Homeland Security
DLA	Driver License Agreement
DLC	Driver License Compact
DL&C	Driver Licensing and Control
DL	Driver's License
DMV	Division of Motor Vehicles
DOB	Date of Birth
DOS	Department of State
DOT	Department of Transportation
DPPA	Driver Privacy Protection Act
DPS	Department of Public Safety
DRIVerS	Driver Record Information Verification System
EVVER	Electronic Verification of Vital Event Records
FDR	Fraudulent Document Recognition
FIPP	Fraudulent Identification Prevention Program
FMCSA	Federal Motor Carrier Safety Administration
HAZMAT	Hazardous Materials
ID	Personal Identification Card
IMDLIS	Improved Driver License Information System
INS	(former) U.S. Immigration and Naturalization Services
ITIN	Individual Taxpayer Identification Number
LE	Law Enforcement

MCSIA	Motor Carrier Safety Improvement Act of 1986
MRT	Machine-Readable Technology
MVA	Motor Vehicle Administration
NCIC	National Crime Information Center
NDR	National Driver Register
NGMV	Next Generation Motor Vehicles
NLETS	National Law Enforcement Telecommunication System
NHTSA	National Highway Traffic Safety Administration
NRVC	Nonresident Violators Compact
OTJ	On-the-Job
OVD	Optical Variable Device
PDF	Portable Document Format
RACF	Resource Access Control Facility
USCIS	United States Citizenship and Immigration Services
USPS	United States Postal Service
USSS	United States Secret Service
SAVE	Systematic Alien Verification Entitlements
SSA	Social Security Administration
SSN	Social Security Number
SSOLV	Social Security On-line Verification
TVDL	Temporary Visitor Driver's License
VDEC	Vehicle Document Examiner Certification Training

BLANK PAGE

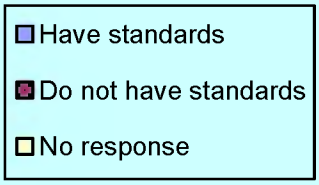
Section A

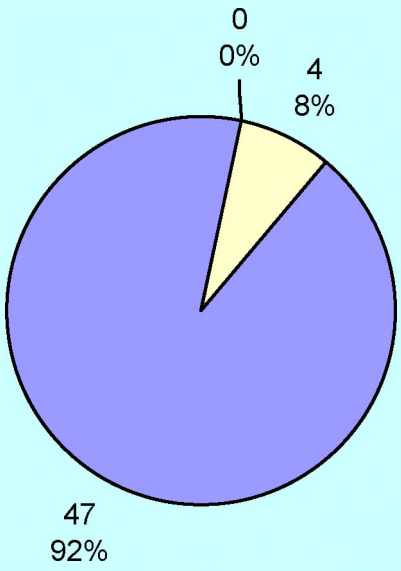
The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

TABLE A-1	Have standards and procedures for providing proof of identity of a DL/ID applicant

Summary: All jurisdictions surveyed indicated they have standards and procedures for providing proof of identity of an applicant for a DL/ID. All jurisdictions utilize a standard list for acceptable documents for proof of identification. Few jurisdictions are utilizing the *AAMVA Security Framework's – Acceptable Verifiable Resource List*. Jurisdictions use a variety of lists for proof of identification. Some jurisdictions continue to utilize the *1996 Uniform Identification – Model Practices*.

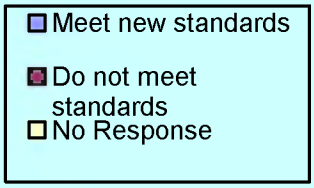


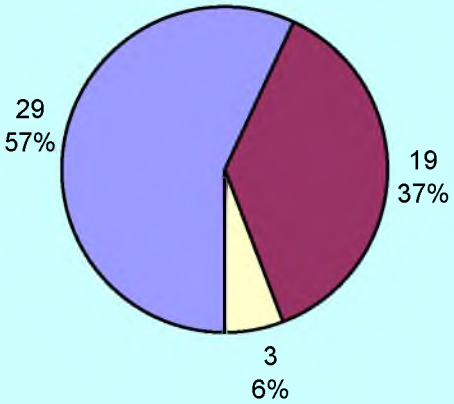


SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

TABLE A-2	Standards and procedures meet or exceed the requirements developed by the DLA and the *AAMVA Security Framework*

Summary: A majority of jurisdictions indicate that they meet or exceed the standards developed by the *AAMVA Security Framework* and the Driver License Agreement. Many jurisdictions responded as meeting the standard but are using the old 1996 standards or similar to. It is difficult to summarize this table due to the variations in interpretations on meeting the newest standards as developed by AAMVA and the DLA.

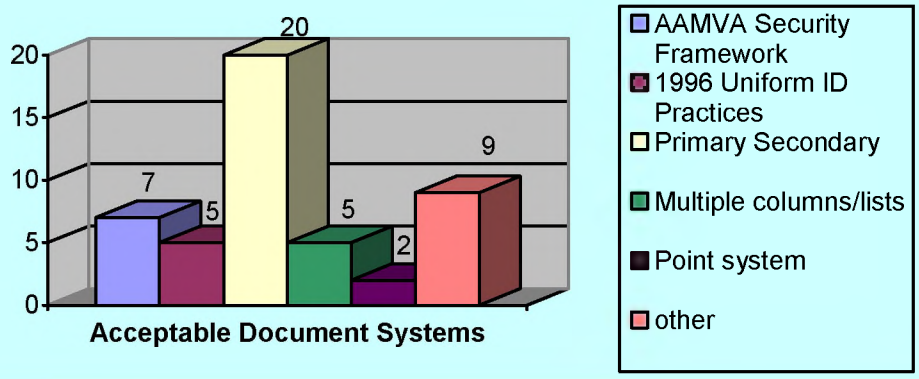




SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

TABLE A-3	Utilize a standard list for acceptable proof of identity documents

Summary: All jurisdictions surveyed indicate they utilize a standard list of acceptable documents. A variety of standardized lists are utilized.



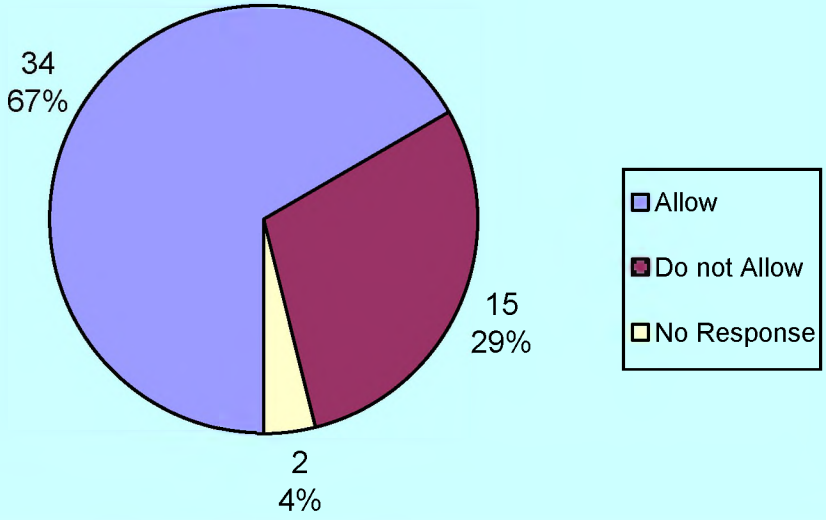
SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

TABLE A-4	Accept foreign documents other than Passports

Summary: A majority of the jurisdictions accept foreign documents, other than a passport, as a form of proof of identification.

Appropriate immigration documentation in conjunction with foreign documents is generally required.

Jurisdictions generally require foreign documents, such as the birth certificate, to be translated.



SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.

TABLE A-5	Procedures for processing an applicant for proof of identify

Summary: The procedures were too lengthy to provide in the telephone interview.

SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.	
TABLE A-6	**Have exception processing for proof of identification procedures**
Summary: Most jurisdictions indicated that they have an exception process for proof of identity. The procedures utilized vary. Most jurisdictions require supervisory approval for exceptions cases.	

SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.	
TABLE A-7	**The minimum standard for proof of identity of an applicant for a driver's license or personal identification card should be:**
Summary: All jurisdictions support the implementation of a standardized list of acceptable documents for proof of identity. Documents should prove (1) name, (2) date-of-birth, (3) Social Security Number and (4) signature. While not agreed upon by all jurisdictions, additional elements could include address and legal presence. Not all jurisdictions feel that the standardized list should be mandated by the federal government. AAMVA could set the standard that jurisdictions would follow. Nearly all jurisdictions feel that the acceptable documents should be verifiable, preferably through electronic means. AAMVA needs to establish a standardized exceptions processing procedure for applicants who cannot meet the identification requirements. A standardized list should be implemented for non-citizens.	

SECTION A: The Act requires the development of standards for documentation to be required as proof of identity of an applicant for a driver's license or personal identification card.	
TABLE A-8	**Comments to assist in the development of minimum standards for proof of identity**
Summary: Most jurisdictions support the AAMVA DL/ID Security Framework and the Driver License Agreement. Online verification systems need to be established and improved for the verification of identification documents used in the establishment of an identity.	

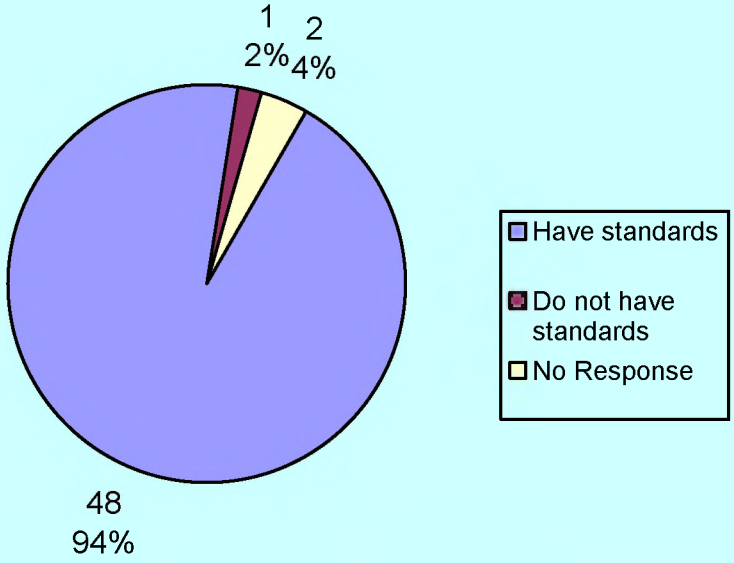
Section B

The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.

TABLE B-1	Have standards and procedures for verifying the documents used to obtain a DL/ID

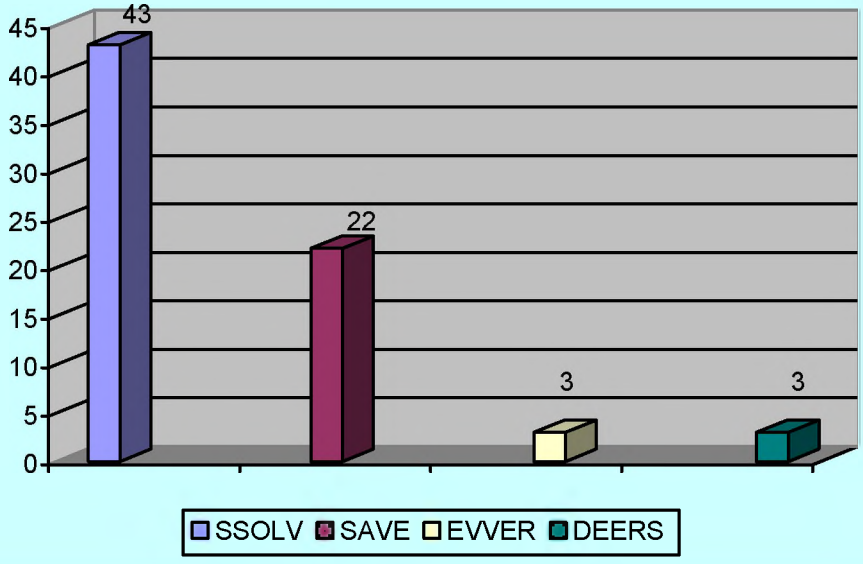
Summary: Most jurisdictions have standards for verifying the documents used to obtain a DL/ID.



SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.

TABLE B-2	Online verification systems currently used (as of February 2005)

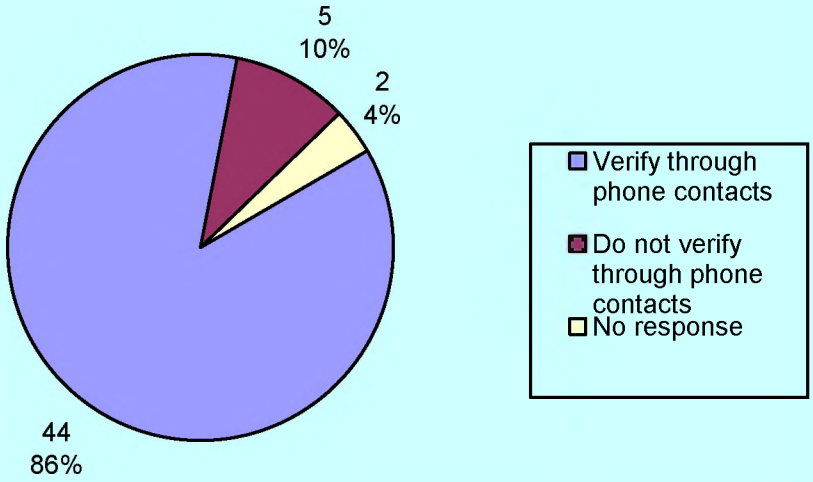
Summary: Most jurisdictions utilize or anticipate utilizing SSOLV. A variety of other systems are also utilized or anticipated. Jurisdictions have issues with the reliability of SAVE and the verification of vital record events.



SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.

TABLE B-3	Verify other types of documents through telephone contacts

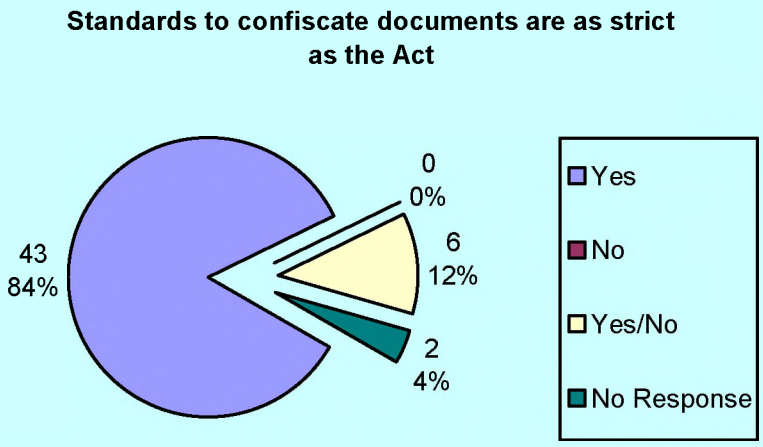
Summary: A majority of jurisdictions verify documents through telephone contacts, usually when processing non-U.S. citizens and when fraudulent activity is suspected. To verify all documents though telephone contacts is too time consuming.



SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.

TABLE B-4	Provide for data sharing between law enforcement and motor vehicle administrations, including but not limited to, exchanges of digital photo and driver records

Summary: Most jurisdictions provide for data sharing between law enforcement and motor vehicle administrations, including but not limited to, exchanges of digital photo and driver records? Some are not permitted to share outside of jurisdictional borders.



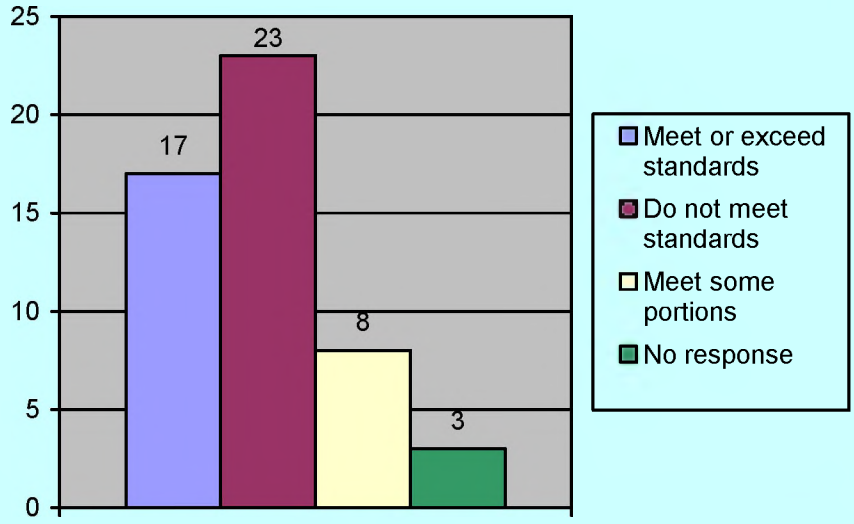
SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-5	**Employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format**
Summary: Roughly, half of the jurisdictions employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format.	

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-6	**Retention period for paper copies of source documents**
Summary: Retention periods for paper copies of source documents varies from none to indefinite.	

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-7	**Retention periods for images of source documents**
Summary: Retention periods for images of source documents various from none to indefinite.	

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-8	**Standards and procedures meet or exceed the requirements developed by the DLA and *AAMVA Security Framework***

Summary: A majority of the jurisdictions do not meet the standards developed in the DLA or the *AAMVA Security Framework*.



SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-9	**The minimum standard for verifiability of documents used for proof of identity for driver's licenses and personal identification cards should be:**

Summary: Most jurisdictions support the *AAMVA Security Framework* and the Driver License Agreement. The jurisdictions feel that real-time, online verification is critical. The correctness of information received from the source is also vitally important.

Improvements must be made to vital records verification. Some improvement need to be made with SAVE and SSOLV. The creation of an all-driver-pointer system is a must for states to be able to verify if a person has been licensed in another state.

Standards need to be set for all online verification systems to interact as effectively as possible.

Jurisdictions should only accept original documents.

SECTION B: The Act requires the development of standards for the verifiability of documents used to obtain a driver's license or personal identification card.	
TABLE B-10	**Comments to assist in the development of minimum standards for verifiability of documents**

Summary: Most states support the *AAMVA Security Framework* and the Driver License Agreement. Need to have online verification systems. States should not have to verify documents that are not capable of accurate online verification. Need to have an all-driver-pointer system.

BLANK PAGE

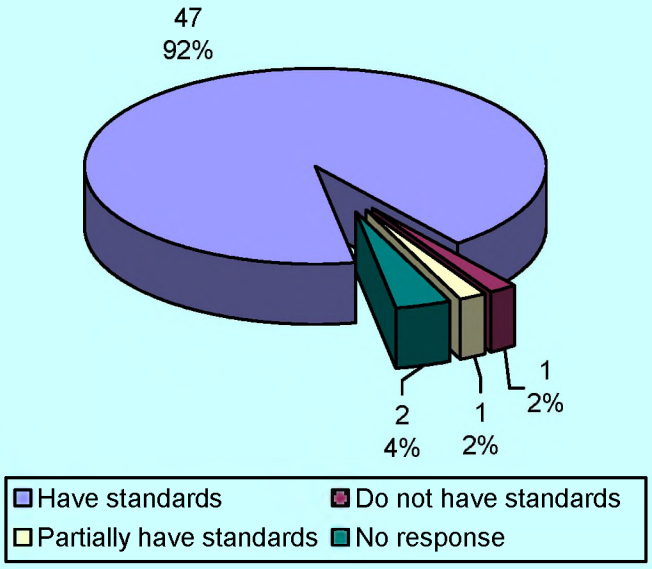
Section C

The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-1	Have standards and procedures for the processing of applications for driver's license or personal identification cards to prevent fraud

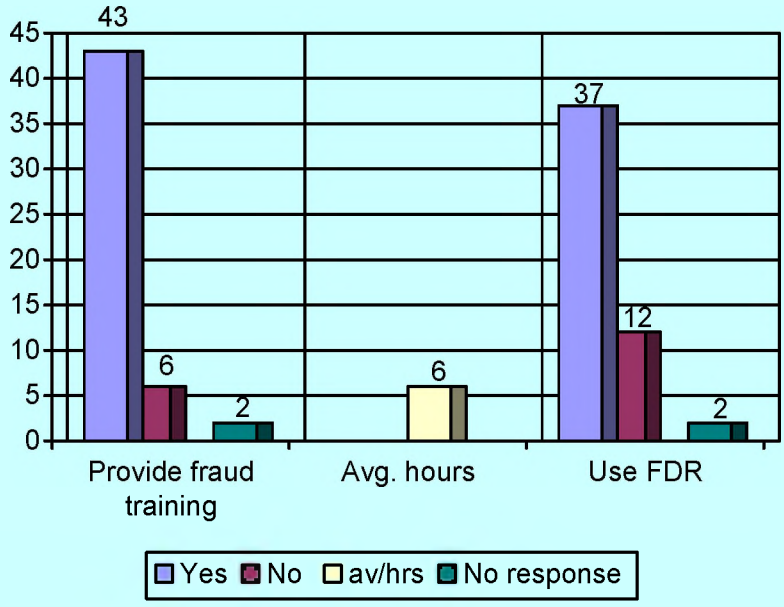
Summary: Most jurisdictions have standards and procedures in place for the processing of applications for driver's license or personal identification cards to prevent fraud.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-2	Provide document fraud training	Number of hours provided for fraud document training	Utilize the AAMVA FDR Model Training Program

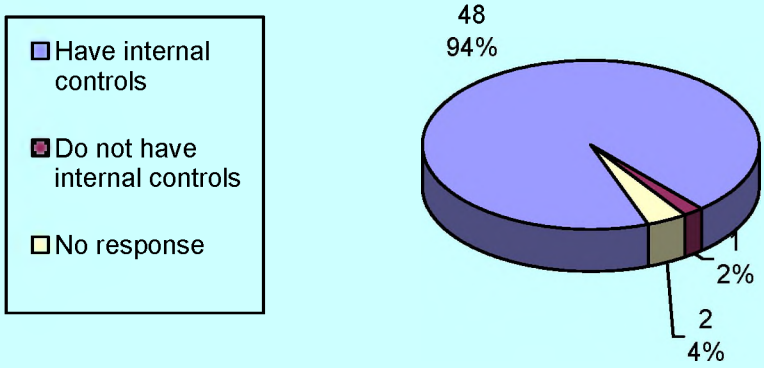
Summary: Most jurisdictions have fraud training in place. The number of hours provided varies greatly and most jurisdictions are utilizing the AAMVA FDR Model.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-3	Have internal controls for business processes

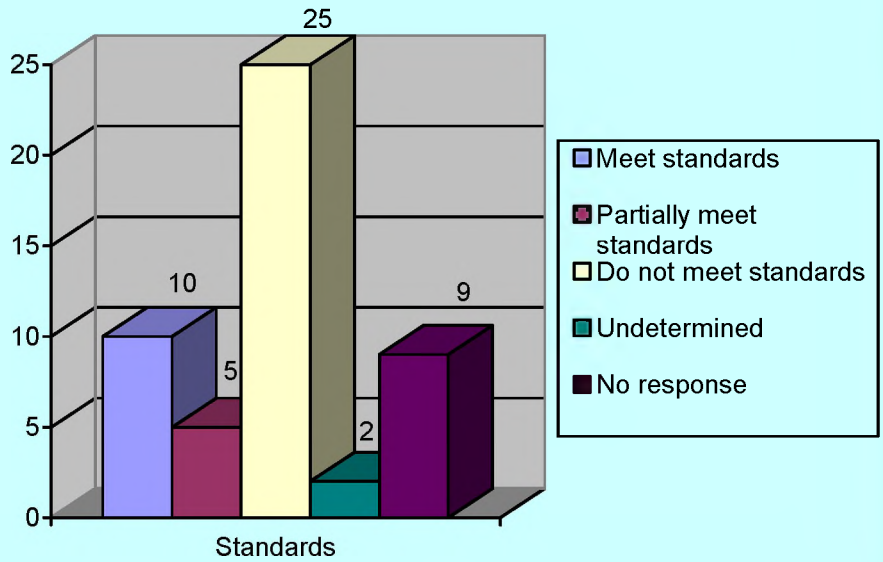
Summary: Most jurisdictions indicated they have some form of internal controls in place. Controls utilized vary.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

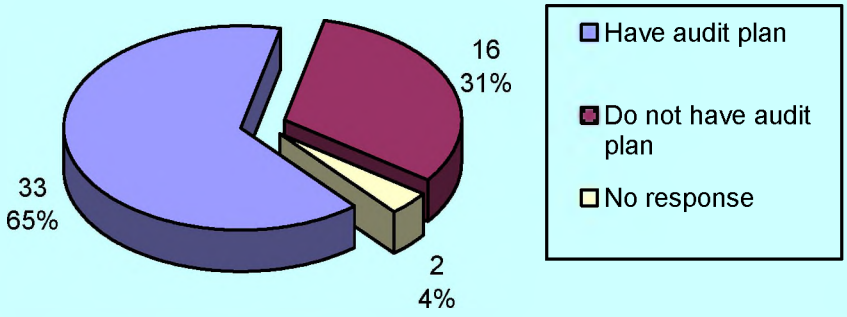
TABLE C-4	Follow the AAMVA standard for internal controls

Summary: Most jurisdictions do not follow the AAMVA standard for internal controls.



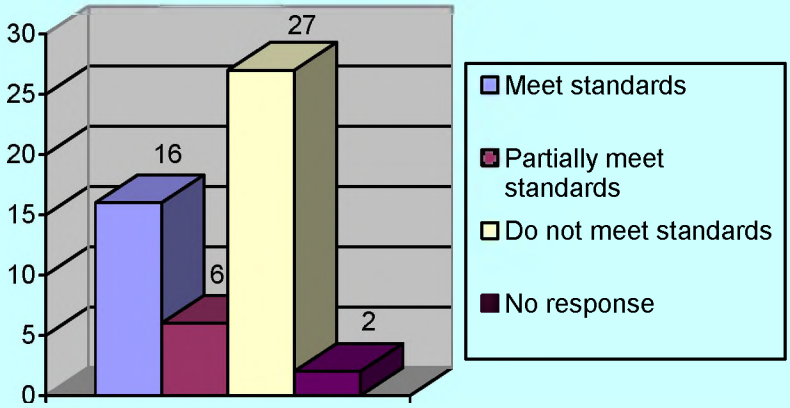
SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-5	**Have an audit plan in place for the DL/ID issuance process**

Summary: Most jurisdictions have an audit plan in place for DL/ID issuance processes.



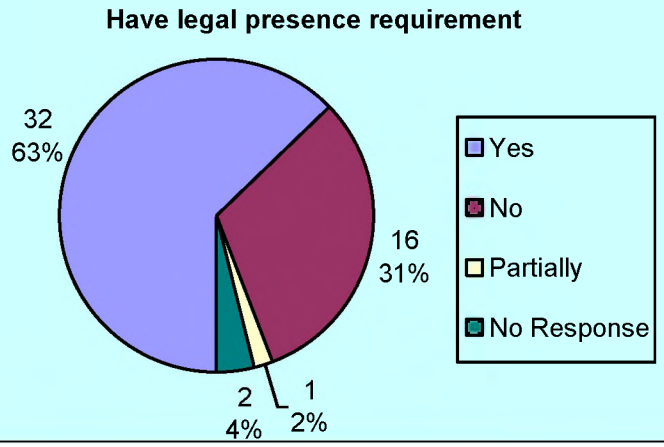
SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-6	**Adhere to AAMVA's name collection use and maintenance procedures**

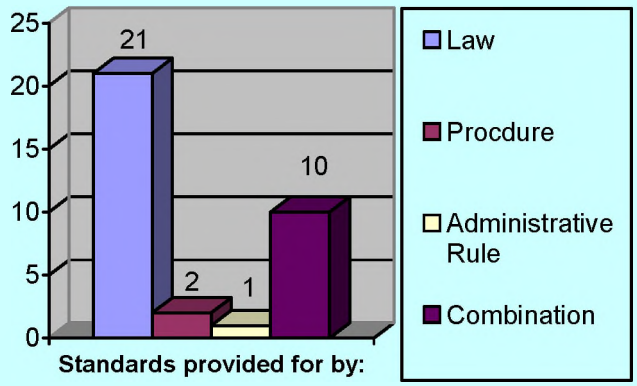
Summary: A majority of jurisdictions do not adhere to the AAMVA name collection and maintenance procedures.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.		
TABLE C-7	**Have legal presence requirement**	**Provided for by: Law, Procedure, Administrative Rule or Other**

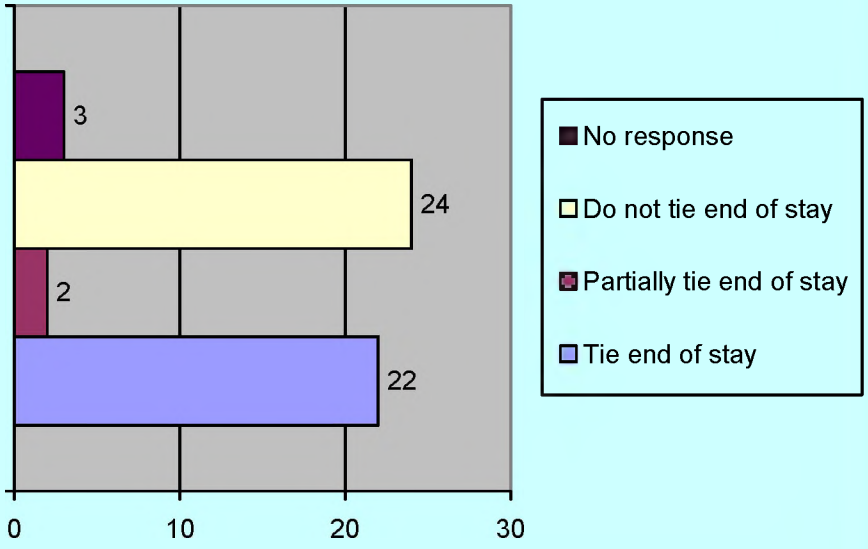
Summary: Most jurisdictions have a legal presence requirement.





SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-8	**Tie end of stay to the expiration date of the DL/ID**

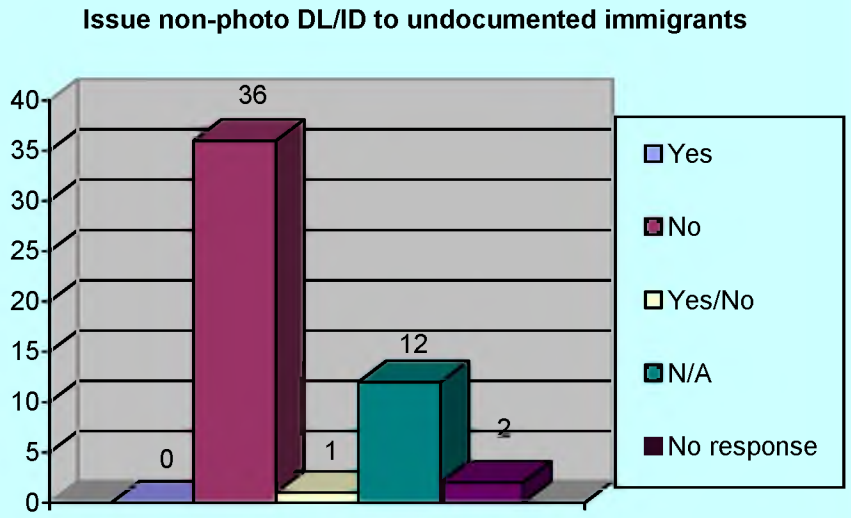
Summary: Most jurisdictions do not tie the end of stay to the expiration of immigration documentation.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-9 — **Issue non-photo DL/ IDs to undocumented immigrants**

Summary: Of those jurisdictions that have a legal presence requirement, most are not issuing non-photo DL/IDs to undocumented immigrants.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-10 — **Issue temporary DL/ID to applicants who present:**

Jurisdiction	valid, unexpired non-immigrant Visa		non-immigrant Visa status form		pending application for asylum		pending or approved application for temporary protected status		approved deferred action status form		pending application for adjustment of status	
	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
	13	33	12	34	12	34	12	34	12	34	15	31

Summary: Most jurisdictions do not issue a temporary DL/ID to applicants who submit out-of-the norm immigration documentation.

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-11 — **Temporary DL/ID is valid for the period of time of the applicant's authorized stay in the U.S.**

Summary: Most jurisdictions do not issue a temporary DL/ID to applicants who submit out-of-the norm immigration documentation. For those that do, the temporary DL/ID is valid for the period of authorized stay or less than.

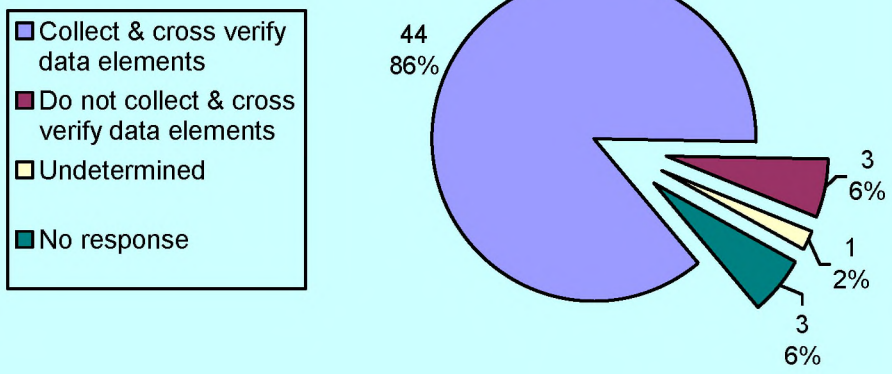
SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-12	**With no definite end to the period of authorized stay, DL/ID is valid for:**
Summary: Validity periods range from 1 to 10 years.	

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-13	**Temporary clearly indicates that it is temporary and states the date on which it expires**
Summary: Yes-10 No-11 N/A-30	

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-14	**Temporary can be renewed only upon presentation of valid immigration documents that the status of stay has been extended by DHS**
Summary: Yes-15 No-5 N/A-31	

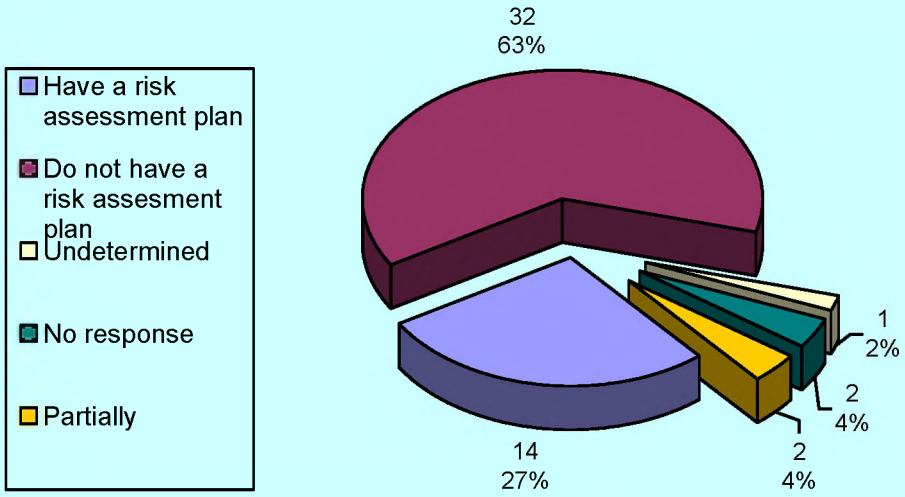
SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-15	**Collect and cross verify data elements**

Summary: A majority of jurisdictions collect and cross verify data elements.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-16	**Have a risk assessment plan**

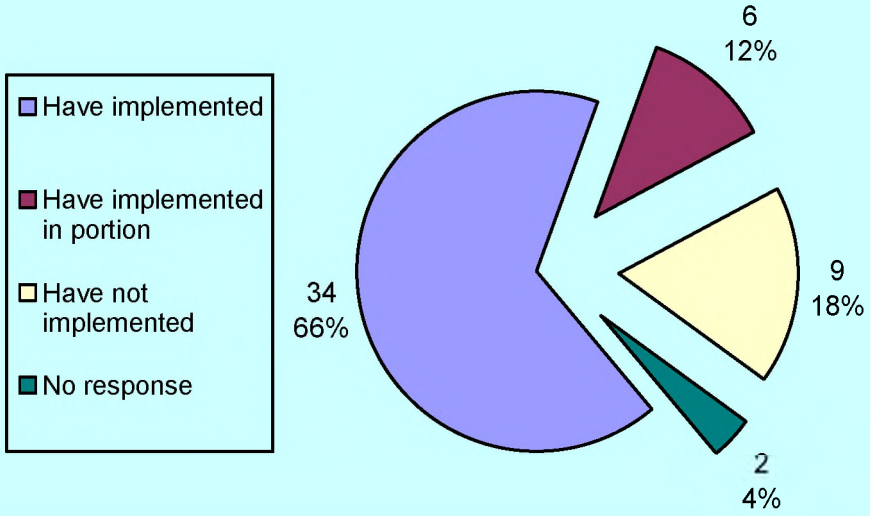
Summary: Most jurisdictions do not have a risk assessment plan. AAMVA should consider developing a model.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

TABLE C-17	Implemented appropriate fraud prevention and detection systems

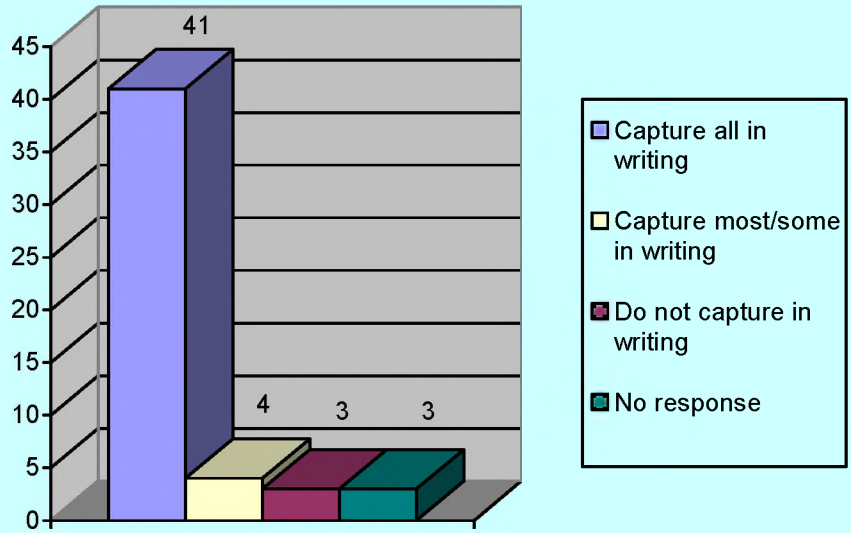
Summary: Most jurisdictions indicate they have implemented appropriate fraud prevention and detection systems.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.

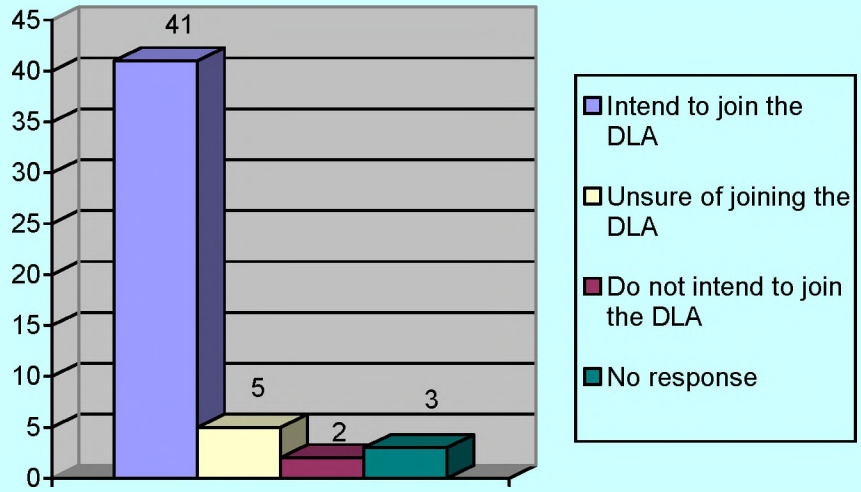
TABLE C-18	Capture all procedures and business processes in writing

Summary: Most jurisdictions indicate they capture all procedures and business processes in writing.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-19	**Intend to become a member of the DLA**

Summary: Most jurisdictions indicate they intend to become a member of the DLA.



SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-20	**Processing standards and procedures meet or exceed the requirements developed by the DLA and AAMVA Security Framework**

Summary: Most jurisdictions do not meet, or partially meet, the processing standards and procedures developed in the DLA and *AAMVA Security Framework*.

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-21	**The minimum standard for the processing of applications for driver's licenses and personal identification cards should be:**
Jurisdiction	

Summary: Most jurisdictions support the *AAMVA Security Framework* and the DLA. Verification processes need to be improved. Biometrics needs to be considered. Jurisdictions should not accept source documents unless they can be verified, either manual or electronically. Jurisdictions should be purse electronic verification where available. They should not be required to verify documents not capable of electronic verification nor be required to utilize systems that have not been certified to proved timely and correct information. Need to have interoperability between all issuing agencies.

SECTION C: The Act requires the development of standards for the processing of applications for driver's license or personal identification cards to prevent fraud.	
TABLE C-22	**Comments to assist in the development of minimum standards for processing applications**
Jurisdiction	

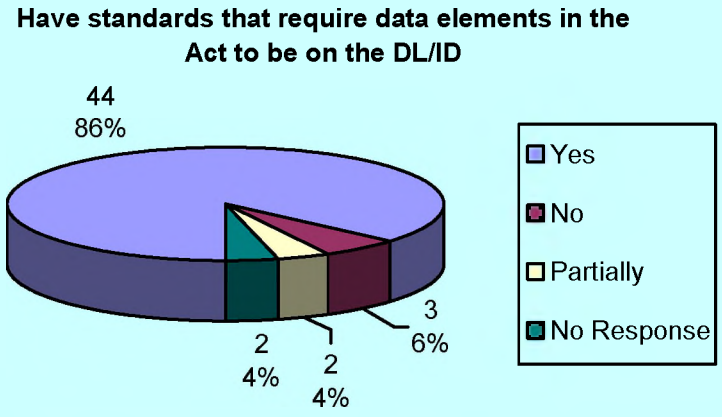
Summary: Need to have appropriate funding to support and time to implement minimum requirements developed. Federal requirements will need to be clearly defined. Need to have online real time verification. Current systems need to be improved and need to resolve the issue of charges for services. The costs are very high for online verification services. FDR training can assist in the verification process.

Section D

The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.

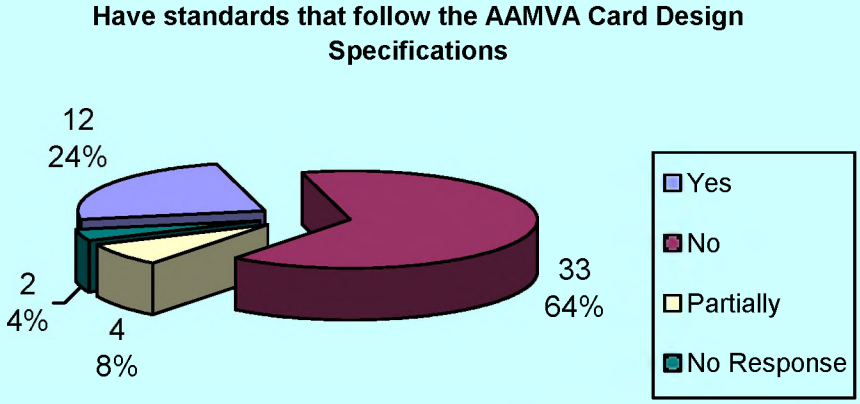
SECTION D:	The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.
TABLE D-1	**Have standards that require the data elements listed to be included on the DL/ID**

Summary: Most jurisdictions have standards that require the data elements listed in the Act to be on the DL/ID. Not all require the full legal name. Some jurisdictions place the mailing address on the face of the document rather that the physical address as they have concerns for safety/security of their constituents.



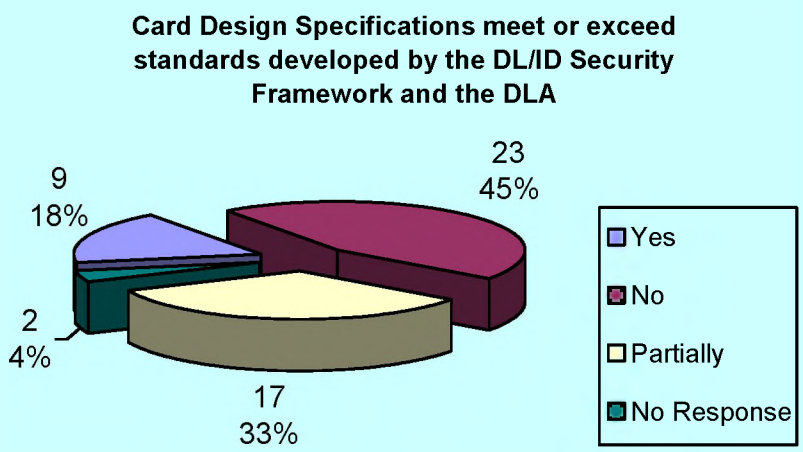
SECTION D:	The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.
TABLE D-2	**Standard follows the AAMVA Card Design Specifications**

Summary: Most jurisdictions do not currently follow the AAMVA Card Design Specifications. Many jurisdictions are preparing RFPs for their new DL/ID contracts and will be migrating to the Card Design Specifications in whole or part.



SECTION D:	The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.
TABLE D-3	**Card Design Standards meet or exceed the requirements developed by the *AAMVA Security Framework***

Summary: A majority of jurisdictions do not meet or exceed the requirements developed by the *AAMVA Security Framework*; however, jurisdictions continue to make improvements.



SECTION D:	The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.
TABLE D-4	**The minimum standard for Card Design Specification for driver's licenses and personal identification cards should be:**
Jurisdiction	

Summary: Most jurisdictions support the *AAMVA Security Framework* and DLA. Jurisdictions have some issues with the *AAMVA Card Design Specifications*. Need to look at biometrics. Could be an indicator for legal presence status.

SECTION D:	The Act requires the development of standards for information to be included on each driver's license or personal identification card, including (i) the person's full legal name, (ii) the person's date of birth, (iii) the person's gender, (iv) the person's license or personal identification card number, (v) a digital photograph of the person (vi) the person's address of principal residence, (vii) the person's signature.
TABLE D-5	**Comments to assist in the development of minimum standards for information to be included on the DL/ID**
Jurisdiction	

Summary: Generally, jurisdictions support the DLA and the *AAMVA Security Framework*. Appropriate funding needs to be provided to meet minimum requirements. Time-frames to implement minimum requirements need to be considered. Jurisdictions have contract cycles that need to be accounted for.

BLANK PAGE

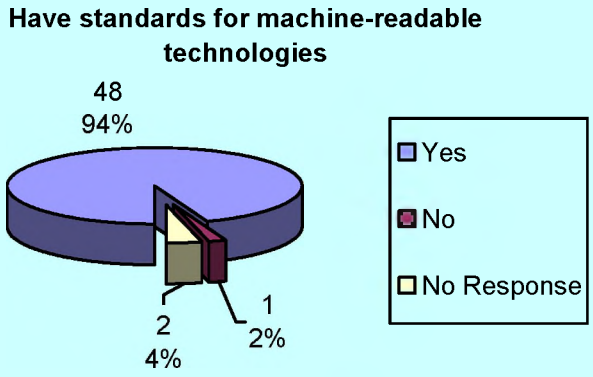
Section E

The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.

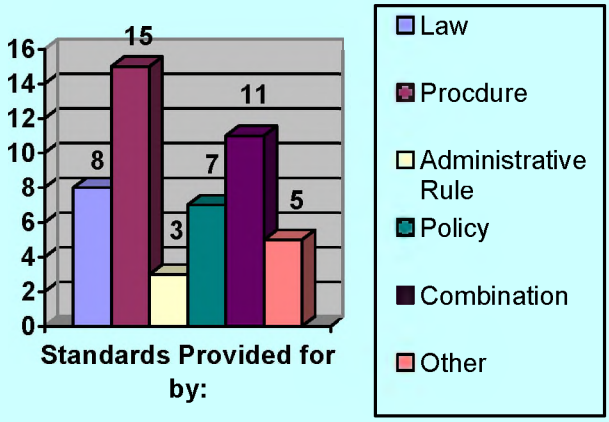
SECTION E: The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.			
TABLE E-1	**Have standards that require common machine-readable identity information to be included on the DL or ID, including defined minimum data elements**	**Provided for by: Law, Procedure, Administrative Rule, Other**	**Machine-readable Technologies**

Summary:

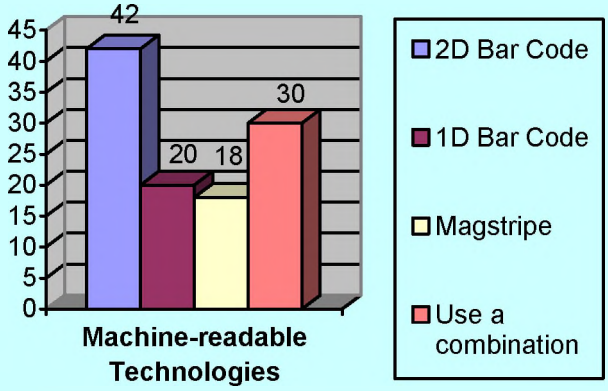
1. Most jurisdictions have standards that require common machine-readable identity information to be included on the DL or ID, including defined minimum data elements.



2. Standards are provided for by a combination of law, administrative rule, policy, procedure and other.



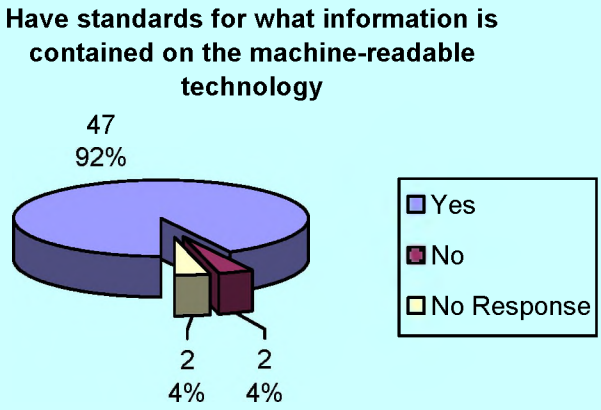
3. 2D and 1D bar codes are the most common MRT, followed by the magstripe. Thirty jurisdictions use a combination of machine-readable technologies.

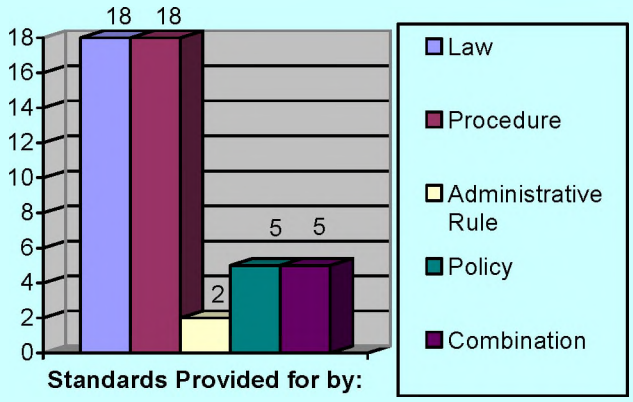


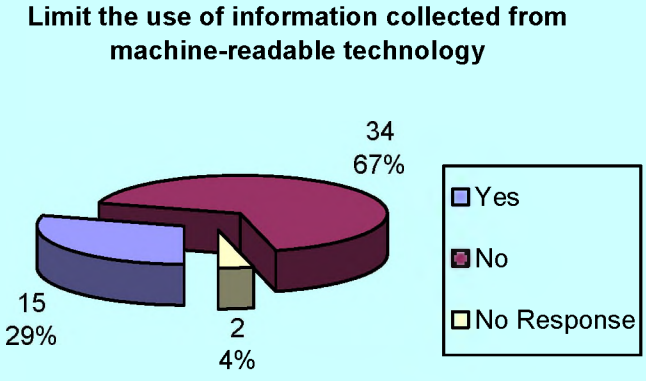
SECTION E: The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.				
TABLE E-2 **Jurisdiction**	**Have a standard for what information is contained in the machine-readable portion of the documents**	**Provided for by: Law, Procedure, Administrative Rule, Other**	**Limit the use of information collected and used from the machine-readable portion(s) of the document**	**Provided for by: Law, Procedure, Administrative Rule, Other**

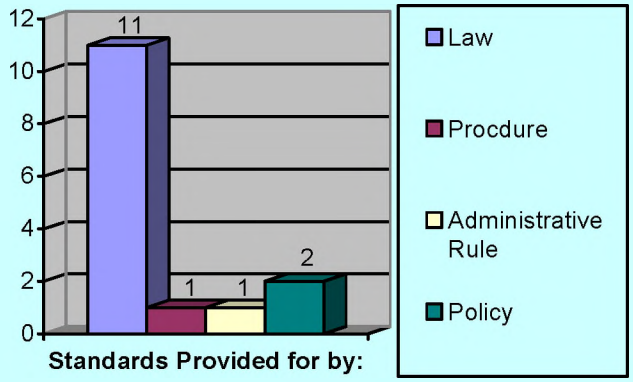
Summary:

1. Most jurisdictions have a standard for what information is contained in the machine readable portion of the documents
2. Standards are provided for by a combination of law, administrative rule, policy, procedure and other.
3. Most jurisdictions do not limit the collection and use from the machine readable portions of the document.
4. For those jurisdictions that do limit the collection and use from the machine readable portions of the document, it is generally provided for by law and policy.



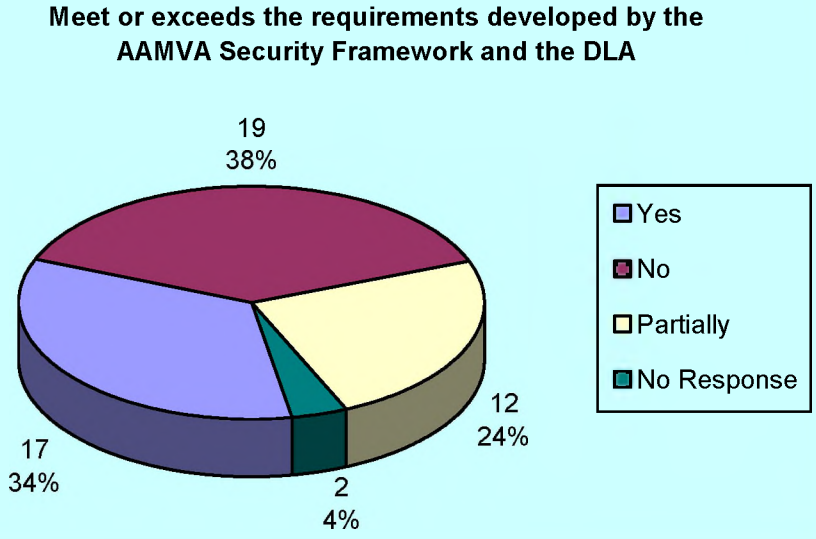






SECTION E: The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.	
TABLE E-3	**Meet or exceed the requirements developed by the DLA and AAMVA Security Framework**

Summary: Most jurisdictions partially meet, meet or exceed the requirements developed by the DLA and *AAMVA Security Framework*, for card design specifications and limiting the use of MRT.



SECTION E: The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.	
TABLE E-4	**The minimum standard for machine readable identity information to be included for driver's licenses and personal identification cards should be:**
Jurisdiction	

Summary: Generally, jurisdictions feel that the minimum standard developed should require the information contained on the front of the document to be stored in the MRT. Jurisdictions generally support the requirements in the DLA and *AAMVA Security Framework*. A number of jurisdictions feel that a biometric should be included and that parts of the MRT should be encrypted or that the document should include an additional MRT that is encrypted.

SECTION E: The Act requires the development of standards for common machine readable identity information to be included on each driver's license or personal identification card, including defined minimum data elements.	
TABLE E-5	**Comments to assist in the development of minimum standards for information to be included on machine readable technologies**
Jurisdiction	

Summary: Generally, jurisdictions feel that the minimum standard developed should require the information contained on the front of the document to be stored in the MRT. Jurisdictions generally support the requirements in the DLA and *AAMVA Security Framework*. A number of jurisdictions feel that a biometric should be included and the parts of the MRT should be encrypted or that the document should include an additional MRT that is encrypted.

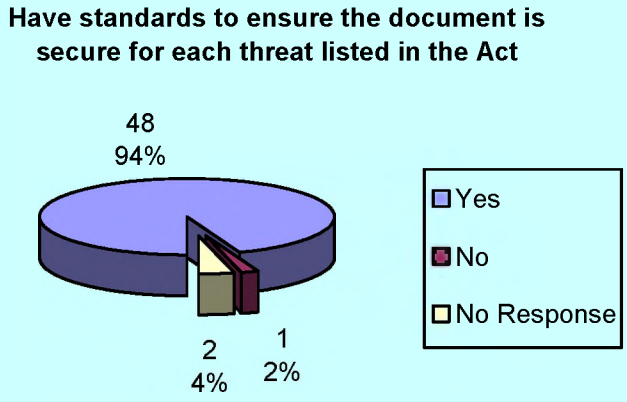
When developing the minimum requirements, DOT needs to consider the costs associated with machine-readable technologies and be prepared to assist the jurisdictions in absorbing the costs.

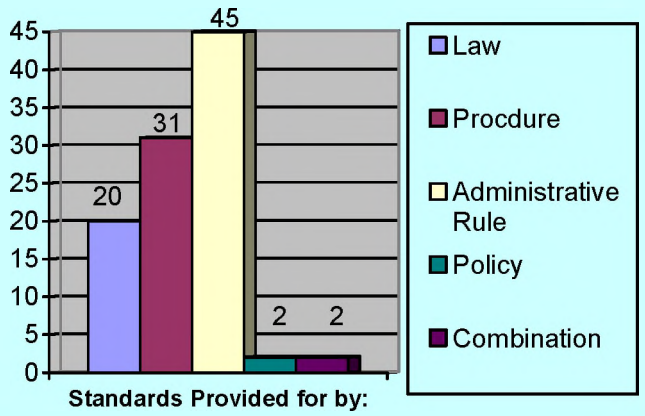
Section F

The Act requires the development of security standards to ensure that driver's license or personal identification cards are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.

SECTION F: The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.		
TABLE F-1	**Have standards that ensure the document is secure for each threat listed in the Act for each DL or ID issued**	**Provided for by: Law, Procedure, Administrative Rule or Other**

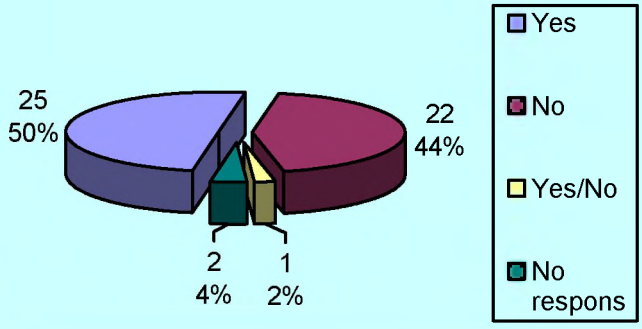
Summary: Almost all jurisdictions have standards that ensure the document is secure for each threat listed in the Act for each DL/ID issued. Standards are provided for through a variety of means.

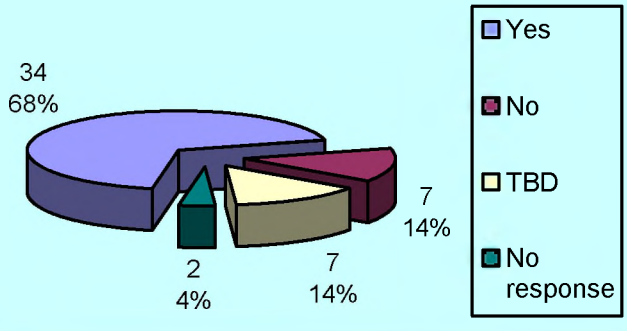




SECTION F: The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.		
TABLE F-2	**Follow the document security requirements as describe in AAMVA Card Design Specifications**	**Planning to introduce the common Level 1 security device (OVD) as developed by AAMVA**

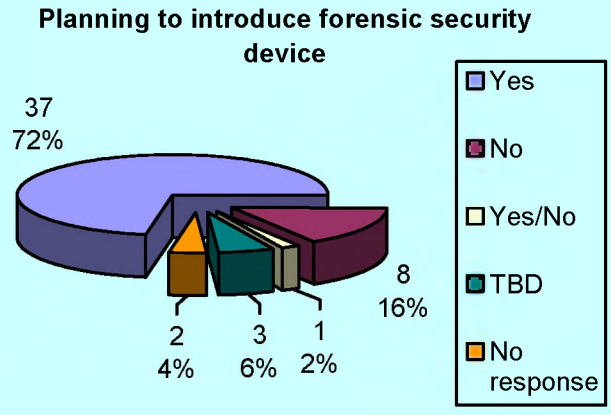
Summary:
1. Roughly, half of the jurisdictions follow the document security requirements as described in *AAMVA Card Design Specifications*.
2. Most jurisdictions are planning to implement the Common Level 1 OVD. Timing is tied to their next contract cycle.

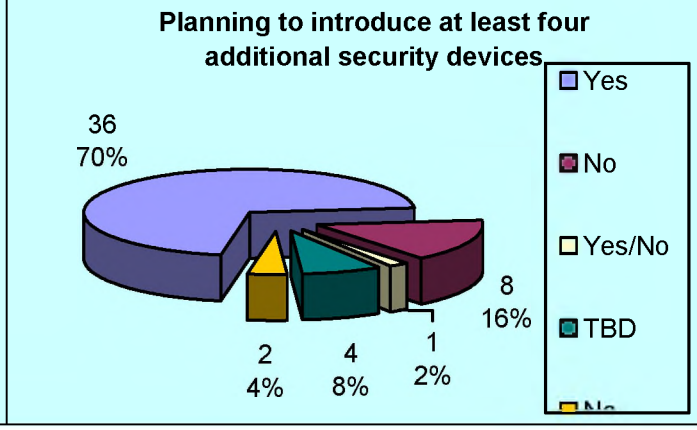




SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.	
TABLE F-3	**Planning to introduce a forensic security device on the document**	**Planning to introduce at least 4 additional security devices (for levels 1 and 2)**

Summary/Conclusion:
1. Most jurisdictions are planning to introduce a forensic security device on the document or have already done so.
2. Most jurisdictions are planning to introduce at least four additional security devices (for levels 1 and 2) or have already done so.





SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.
TABLE F-4	**Period of validity for DL/IDs issued**

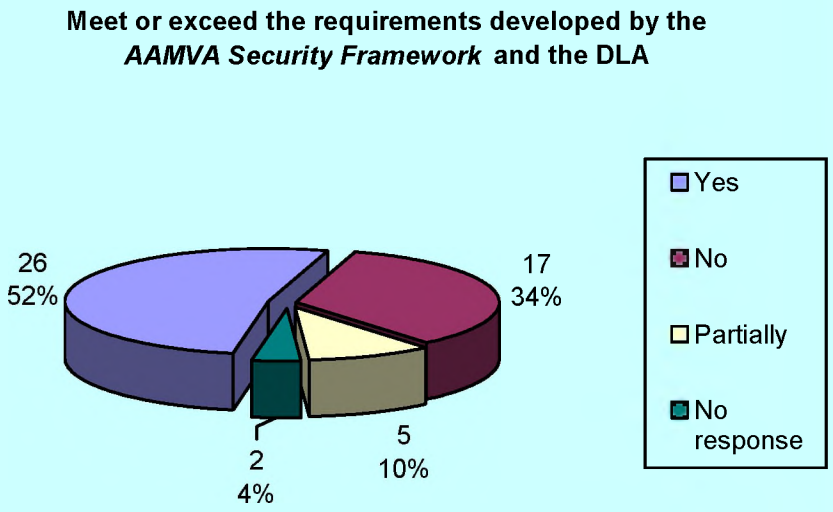
Summary: DL/ID issuance periods range from two to ten years.

SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.	
TABLE F-5	**Allow renewal by mail**	**Allow renewal by internet**

Summary:
1. Most jurisdictions allow for renewal by mail every other cycle.
2. Roughly, half of the jurisdictions allow for renewal by internet every other cycle.

SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.
TABLE F-6	**Meet or exceed the requirements developed by the DLA and *AAMVA Security Framework***

Summary: More than half of the jurisdictions meet or exceed the requirements developed by AAMVA in the DLA and *AAMVA Security Framework*.



SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.
TABLE F-7	**The minimum standard for document security for driver's licenses and personal identification cards should be:**
Jurisdiction	

Summary: Generally, the states support the *AAMVA Security Framework* and the DLA for minimum standards for document security for driver's licenses and personal identification cards.

SECTION F:	The Act requires the development of security standards to ensure that driver's license or personal identification card are; (i) resistant to tampering, alteration, or counterfeiting, (ii) capable of accommodating and ensuring the security of a digital photograph or other unique identifier.
TABLE F-8	**Comments to assist in the development of minimum standards for information to be included on machine-readable technologies.**
Jurisdiction	

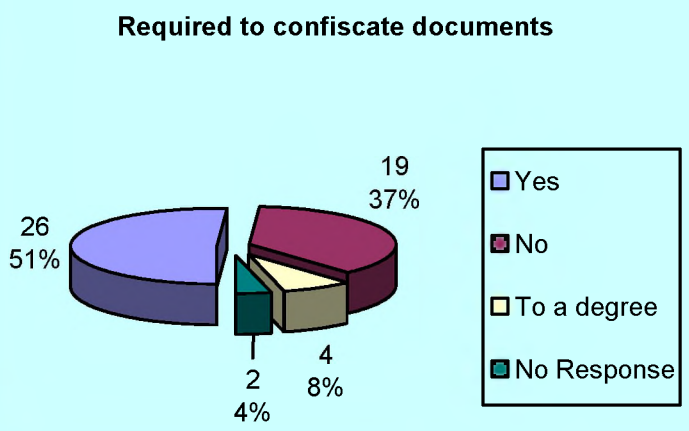
Summary: DOT will need to provide sufficient funding for document security. Additionally, reasonable time-frames will be required given jurisdictional contract periods.

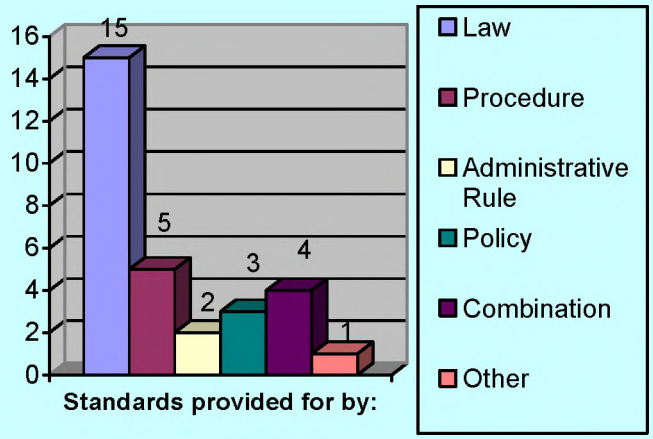
Section G

The Act requires that a state confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.

SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.		
TABLE G-1	**Require confiscation of DL or ID if any component or security feature is compromised**	**Provided for by: Law, Procedure, Administrative Rule or Other**

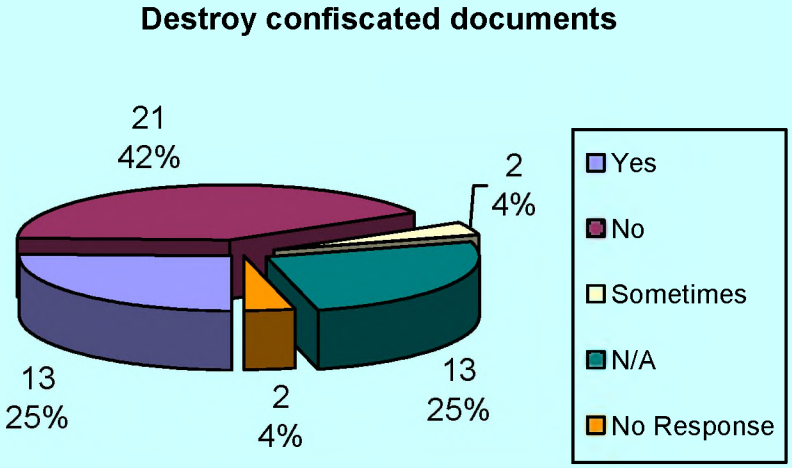
Summary: Roughly, half of the jurisdictions are required to confiscate the DL/ID if any component or security feature is compromised. Some jurisdictions are only authorized to confiscate their own documents. Some jurisdictions turn the documents immediately over to LE or work cooperatively with LE in the MVA offices.





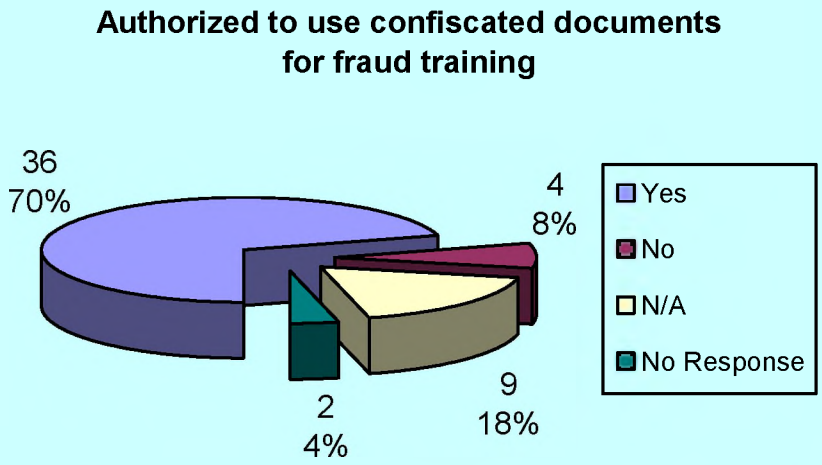
SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-2	**Confiscated documents are destroyed**

Summary: Of those jurisdictions that do confiscate documents, most indicated that they do not destroy the documents. Almost all jurisdictions indicated that they turn the documents over to LE or an internal investigative unit for evidence and prosecution. Almost all jurisdictions who confiscate indicated they try to use the documents of fraud training purposes when the documents are no longer needed for evidence and prosecution. Roughly a quarter of the jurisdictions destroy the documents if not used for fraud training purposes.



SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-3	**Authorized to use confiscated documents for training**

Summary: Almost all jurisdictions that confiscate documents are authorized to use the documents for fraud training purposes. A number of jurisdictions expressed concerns that if the act requires documents to be confiscated, that they also be authorized to be used for fraud training purposes.

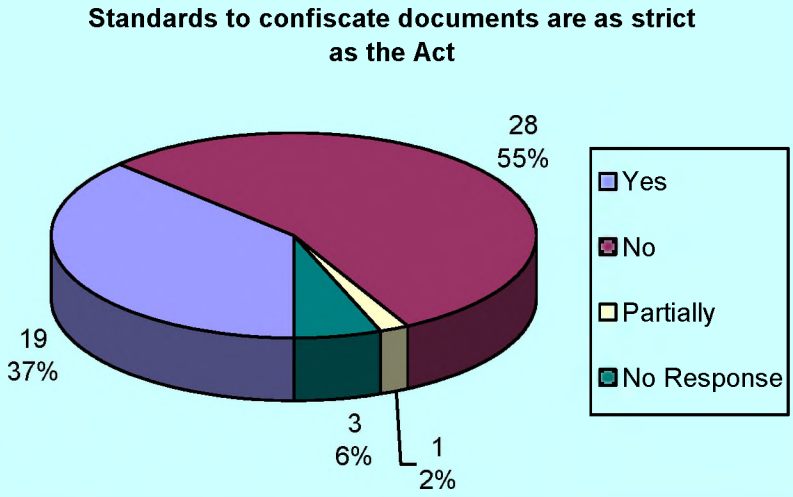


SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-4	**Procedure used if not authorized to confiscate compromised documents**

Summary: Generally, LE can confiscate documents. Jurisdictions that cannot confiscate documents usually make photo copies of the documents and return them to the customer if they do not flee. They then create a record in the system to prevent the person (documents) from attempting a transaction at another DMV office.

SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-5	**Standards and procedures are as strict as the requirements in the Act**

Summary: Less than half of the jurisdictions have standards and procedures as strict as the requirements in the Act.



SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-6	**The minimum standard for confiscating driver's license or personal identification cards that have been compromised should be:**
Jurisdiction	

Summary: Jurisdictions generally support the concept of confiscating documents. However, states feel they should be authorized, but not required, by federal law to confiscate documents. There are circumstances in which the DMV employees would be at risk if they are required to confiscate documents. Due process must also be considered for the applicant. Although the documents or the customer may be suspicious, this does not indicate the person is guilty of committing fraud.

SECTION G: The Act requires that a State confiscate a driver's license or personal identification card if any component or security feature of the license or identification card is compromised.	
TABLE G-7	**Comments to assist in the development of minimum standards for the confiscation of compromised documents**
Jurisdiction	

Summary: DOT should consider the confiscation of all identification documents. DOT needs to authorize jurisdictions to utilize confiscated documents for fraud training purposes.