

http://www.eff.org/files/filenode/realid/real_id_final_rule_part1_2008-01-11.pdf Comparative Analysis of the Provisions of the Driver License Agreement (DLA) the Existing Compacts (DLC, NRVC) and the Real ID Act

PART I: COMMON PROVISIONS

PRINCIPLE/PROVISION	DLA ¹	DLC ²	NRVC ³	DLA Reference	Real ID Act ⁴
One state-issued driver license recognized by all other states.	Yes	Yes, but "Driver License" is not defined in DLC.	No, because "Driver License" is defined as any license or privilege to operate a motor vehicle issued under the law of the home jurisdiction.	General purpose clause, par. 1 Article I(A) par. 13	Yes S. 202(d)(6) NPRM-S. 37.33(c)
One Driver Control Record (DCR)	Yes	No	N/A	General purpose clause, par. 1 Article II(G) and (J)	No
One Jurisdiction of Record (JOR) to maintain one Driver Control Record.	Yes	No, because the concept of JOR does not exist in DLC. The DLC refers to "home state of licensee," and defines it as the jurisdiction that has issued a driver license to a person.	N/A	Article I(A) par. 12 Article II(G) and (I)	No
Definition of "conviction" includes judgments by default or in absentia.	Yes	No	N/A	Article I(A), par. 5	N/A
Definition of "failure to comply" includes failure to answer a citation as well as failure to pay fines, penalties and costs related to a violation.	Yes	No	No NRVC does not address "failure to pay"	Article I(A), par. 8	N/A
Definition of jurisdiction includes "territory or province of Canada as well as any state of Republic of Mexico or Federal District of Mexico."	Yes	No	Yes NRVC defines "jurisdiction" to include "provinces of Canada or other countries."	Article I(A), par. 11	No, Canada and Mexico are not referenced by the Real ID Act.
Licensing authority shall not issue a driver license to an applicant unless jurisdiction has utilized a recognized verification process for purposes of establishing identity (one identity).	Yes	No	N/A	General purpose clause, par. 4 Article II(A)	Yes. Real ID contains extensive prescriptive requirements in this area S. 202(c) NPRM-S. 37.11 See Part II

¹ Final Draft of the DLA as sent to all AAMVA jurisdictions with the ballot dated June 8, 2005.

² Current membership includes all states except Georgia, Massachusetts, Michigan, Tennessee and Wisconsin.

³ Current membership includes all states except Alaska, California, Michigan, Montana, Oregon and Wisconsin.

⁴ References are to the Real ID Act of 2005 which is codified as a note to 49 USC section 30301, and to the Notice of Proposed Rulemaking issued by the U.S. Department of Homeland Security (DHS) on March 1, 2007.

Each applicant shall furnish acceptable proof of identity using documents from the "Acceptable Resource Lists which must be verified either electronically in the case of SSN or by other means such as visual screening."	Yes	No	N/A	Rules for Article II – Appendices II-A and II-C	Yes, same concept, but Real ID has a shorter documents list than the DLA, at the same time that it requires source verification of several identification documents besides a social security card and social security number (SSN). S.202(c) and (d) NPRM-Ss. 37.11 and 37.13 See Part II
Licensing authority shall not issue a driver license to an applicant if existing license has been withdrawn by another jurisdiction for convictions or administrative actions, as well as failures to comply, relating to highway safety and federal mandates.	Yes	No DLC does not deal with administrative actions, although "administrative per se" are allowed in the Administrative Procedures of DLC. In addition, convictions are not limited to matters related to highway safety and federal mandates.	No NRVC applies to moving traffic violations which alone do not carry suspension or revocation. However, there is no precise definition of "traffic violation" in the Compact. Article VIII specifically excludes parking or standing violations, highway weight limit violations and violations governing the transportation of hazardous materials.	General purpose clause, par. 3 and 5 Article II(B)	No, the Real ID Act does not address and therefore does not preclude the issuance of a license to an individual whose license or privilege to drive has been suspended or otherwise withdrawn for cause by another State.
Licensing authority shall not issue a driver license to an applicant unless applicant surrenders existing license.	Yes	Yes	N/A	Article II(F)	Yes, and in addition, there must be confirmation from the former jurisdiction that the surrendered DL/ID card has been terminated. S. 202(d)(6) NPRM-S. 37.33
License authority <u>may</u> issue a driver license to an applicant after the expiration of <u>5 years</u> from effective date of most recent withdrawal.	Yes	No DLC provides that licensing authority may issue a driver license if the revocation of the applicant's license has been in effect for more than <u>1 year</u> . DLC is more permissive on this issue than the DLA.		Article II(C)	N/A
Licensing authority <u>may</u> issue a driver license to an applicant in the case of a withdrawal for failure to comply if it is satisfied that the applicant has made all reasonable efforts to comply but has been unable to do so.	Yes	No	No	Article II(D)	N/A

If a person has not been issued a driver license, the jurisdiction of the person's address shall create and maintain a record, until such time as another jurisdiction shall issue a driver license.	Yes	No Applicant shall submit an affidavit of non-licensure which may take the place of surrendered license.	N/A	Article II(H)	No. Real ID has no provisions concerning records or access to the records of persons who do not have a license or ID card (either because a person has never been issued a DL/ID card or a valid DL/ID card is no longer being held).
Jurisdiction of Record shall give the same effect, in accordance with its laws, to DLA Code convictions and administrative actions which occurred in another jurisdiction as if these convictions and administrative actions had occurred in the JOR.	Yes Unlike the DLC, the DLA makes no distinction between "mandatory convictions" and any other convictions.	Yes This basic principle in the DLA is essentially the same as in the DLC.		Article II(K)	N/A
Except as specified for failures to comply, a jurisdiction may maintain its own driver records on any person and take the withdrawal actions permitted by its laws on any conduct occurring within that jurisdiction.	Yes. However such withdrawals shall not be sent to other jurisdictions. Only DLA Code convictions and administrative actions are sent to the JOR.	Yes	N/A	Article II(M)	N/A
The JOR shall transfer the Driver Control Record within 30 days of receipt of notification of the issuance of a driver license.	Yes	Yes Administrative Procedures of DLC provide for a delay of 30 days.	N/A	Article II(I)	N/A
Following expiration of withdrawal, another jurisdiction may issue a license notwithstanding requirements in the former JOR for alcohol or any rehabilitation or proof of financial responsibility. However, all reinstatement fees in the former JOR must have been paid.	Yes	No	N/A	Article II(L)	N/A
Identity cards issued by a member jurisdiction shall meet the security standards required for driver licenses and require the same proof of identity process as for driver licenses.	Yes	No	N/A	Rule for Article II- Appendices II (A) and II (C) Article III	Yes. Real ID treats ID cards in the same manner as licenses.
Member jurisdictions shall assure its employees have completed the AAMVA Fraudulent Document Recognition Training Program to recognize and detect fraud.	Yes	No	N/A	Article IV, par. 1 Rules for Article IV – section I	No, but see Part II. S. 202(d)(9) NPRM-Ss. 37.41(b)(4)(i)

Member jurisdictions shall develop internal controls to reduce fraud, including a formal audit plan and procedure, as a deterrent to fraud.	Yes	No	N/A	Article IV, par. 2 Rules for Article IV – section 2, Appendix IV- A	Yes, in effect, see Part II. S. 202(d)(7) and (8) NPRM- S. 37.41 Real ID contains additional facilities security requirements-See Part II.
Member jurisdictions shall incorporate certain security and design elements into each license and identification card (i.e., OVD, common machine readable and human readable technology).	Yes	No	N/A	Article IV, par. 4 Rules for Article IV – section 3	Yes, but Real ID contains numerous detailed, prescriptive requirements for card security and design. S. 202(b) NPRM-Ss. 37.15, 37.17 and 37.19 See Part II
Two categories of member jurisdictions: -“ <u>pending member</u> ” – declaration of intent to join within 5 years -“ <u>full member</u> ” – notice of joinder accepted.	Yes	No	N/A	Article V (A) – par. 1 to 6	N/A
Members have power to establish dues, elect officers, amend the Agreement and adopt rules and bylaws.	Yes	Yes	Yes	Article V (A) (7)	N/A
Agreement administered by a Board composed of a Chair, Vice-Chair, immediate past Chair and a representative of each of the regions as defined by AAMVA.	Yes	Yes Joint Executive Board for both Compacts since 1993.	Yes Joint Executive Board for both Compacts since 1993.	Article V (B) (1)	N/A
Board has the power to establish and amend the DLA Code, monitor compliance, resolve disputes, impose sanctions, approve exceptions to the Agreement, determine substantial similarity of state laws to DLA Code and officially interpret the Agreement.	Yes	No	No	Article V (B) (2)	N/A
Amendments to the Agreement are executed by ballot and must be approved by at least 2/3 of member jurisdictions in good standing.	Yes	No The DLC has no amendment clause.	No The NRVC requires unanimous endorsement of all party jurisdictions to amend the Compact.	Article VII	N/A
In case of failure to comply, the jurisdiction that issued the citation <u>shall</u> not withdraw the driver license and shall notify the JOR. Only the JOR is authorized to withdraw the Driver license.	Yes	N/A	No The NRVC states that the issuing jurisdiction <u>need</u> not suspend the privilege of a driver for whom a report has been transmitted to the home jurisdiction.	Article IX (D) and (E)	N/A
In case of failure to comply, a withdrawal shall continue until the JOR receives satisfactory evidence of compliance.	Yes	N/A	Yes	Article IX (E) Exception: article II (D)	N/A

No notification of failure to comply shall be transmitted to the JOR more than 6 months after the date the court, tribunal or agency determines the person has failed to comply.	Yes	N/A	Same time period (i.e., 6 months) but different starting date. NRVC refers to "six months after the date on which the traffic citation was issued."	Article IX (F)	N/A
The JOR must give the same effect to convictions and administrative actions reported to it from a member jurisdiction, as if the conduct occurred in the JOR.	Yes	Yes	Yes	Article X (A)	N/A
Licensing authority has 30 days to report convictions and administrative actions to the JOR, electronically or by the other means.	Yes	No But Administrative Procedure of DLC require a jurisdiction to report each conviction to the home jurisdiction within 15 days after receipt of conviction from the court.	N/A	Article X (B)	N/A
An electronic copy of a record transmitted and received of any conviction, administrative action, driver license and identification card issuance, withdrawal or driver status is admissible in evidence in all courts and administrative proceedings without further proof.	Yes	No	No	Article XI	No, even though Real ID requires electronic exchange among States and mutual electronic access – see Part II – it makes no provision for use of electronic records in legal proceedings.
A member jurisdiction may propose exceptions to compliance that are not detrimental to the underlying principles of the Agreement in its "Notice of Joinder" or at a later time. Exceptions are valid for up to 5 years. However exceptions to paragraph 4 of Article IV may be valid for up to 12 years.	Yes	No	No	Article XII	N/A
Provisions of the Agreement are severable and shall be liberally construed.	Yes	Yes	Yes	Article XIII (A) and (B)	N/A
Agreement does not create rights for a driver or other person or a standard of care in any legal or evidentiary sense. Any violation of the Agreement shall not be a defense in any proceeding.	Yes	No	No	Article XIII (C)	N/A

Privacy requirements for data access and exchange, and corrections to records	Yes, but requirement is limited to compliance with existing laws.	No	No		Yes, compliance requires that the State security plan include a "privacy policy regarding personal information collected and maintained by the DMV." However, there is no such requirement stated with respect to third parties that may be involved with the state-to-state exchange of data or the electronic queries to federal databases that are mandated.
---	---	----	----	--	---

PART II: COMPARISON OF KEY SECURITY PROGRAM ELEMENTS

REQUIREMENT	DLA	REAL ID
Maximum DL/ID Card Term	No Requirement.	8 years
Legal Presence	A tie between card expiration date and the end of stay date is "recommended." Categories of non-citizens are defined and additional documents and scrutiny "may" be required.	Applicant must prove legal presence in one of nine (9) specified classifications. Expiration date and end of stay date must be tied in five (5) of the classifications.
Verification of Applicant Identity - Document Requirements -Electronic Verification	Must "utilize a recognized verification process." Rules require the use of the U.S. "Verifiable Resource List" (a/k/a the "Matrix"). Electronic source verification "when available."	The only foreign document that can be accepted is an official passport. Applicant must present at least one of nine (9) specified documents. At least one document must show date of birth. Applicant must show documentary evidence of social security number (SSN). Applicant must show two (2) documents to verify address, which must be recent as specified in the regulation. Every non U.S. citizen must present evidence of lawful status. Exceptions are permitted but must be flagged in both manual and electronic backup files. Exceptions must be fully documented and States must file quarterly reports with DHS. Each U.S. birth certificate must be verified on the EVVE system, or DHS approved alternative. U.S. passport and consular reports must be verified through existing U.S. Department of State's system. Immigration documents must be verified using the SAVE system or DHS approved alternative. Prior DL/ID cards must be verified with States of issuance. SSNs must be verified using the SSOLV system. Addresses must be checked "in accordance with a system of document verification acceptable to DHS."
Name Verification	"Full legal name" must be obtained. Must collect and store "base name record" (a/k/a "name history") and must consult this record when performing all subsequent transactions.	"Full legal name" must be obtained. This term is defined in the NPRM but there are no additional requirements, except that a change of name cannot be made without presentation of an official U.S. or State-issued document, and except that the MRZ (bar code) is supposed to "permit" capture of "the full name history, including full legal name and all name changes."

<p>Document Requirements</p> <p>-Card Material</p> <p>-Card Design</p> <p>-Card Security Features</p> <p>-Machine Readable Zone (MRZ)</p> <p>-Source Document Retention</p>	<p>No Requirement</p> <p>There are minimum mandatory data elements, to which States are free to add. There is a comprehensive scheme for zone placement of mandatory and optional data elements.</p> <p>Each DL/ID card must have a minimum of four (4) security features. These must cover all threat types identified in the “physical security standards” made part of the rules. The rules also incorporate a “DL/ID security device index” to enable member jurisdictions “to make educated decisions about security design.”</p> <p>Two dimensional bar code (PDF417) is minimum, mandatory MRZ technology for all compliant DL/ID cards. There are mandatory and optional data elements.</p> <p>No specific requirement</p>	<p>All card stock must meet specified requirements. Card stock must be UV dull or possess a controlled UV response. Card stock must possess a security background pattern. Card stock must be serialized. Card stock must be highly durable and must have an eight (8) year card life. Card stock must provide for the highest clarity of information applied. Card stock is multi-layered, there must be sufficient adhesion and/or tamper evident properties.</p> <p>Seven (7) personal data elements are mandatory. There are five (5) specific performance requirements for the DL/ID card picture (digital image). Data elements must be printed in roman alphabet characters and the name field must contain no less than thirty-nine (39) characters. Address must appear on the face of the license unless the address is protected or confidential. States must conduct an annual review of their card designs, which must be addressed in the annual report to DHS.</p> <p>Security features must not be reproducible using commonly available technologies. Security features must be layered. There must be at least three levels of elevated security features. Security features must include intricate, fine line multi-colored background; optical variable feature to protect against copying; ultra-violet long wave responsive feature; laser engraving of some variable data; a series of check digit letters or numbers; and covert taggants and/or markers. DL/ID cards must contain all revision dates. States must submit sample DL/ID cards to DHS. States must submit to DHS a lab analysis that addresses eight (8) performance standards with respect to resistance to alteration or counterfeiting.</p> <p>Same requirement as DLA, except that the contents of the bar code must include expiration date, holder’s name, including 125 characters to include full name history, issue date, date of birth, gender, address, DL/ID card number, most recent document revision date and the inventory control number of the card.</p> <p>Paper copies must be retained for at least seven (7) years and electronic or optical copies must be retained for at least ten (10) years.</p>
<p>Production Materials and Facilities Security</p>	<p>The rules state that production “should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. Centralized card production and personalization is recommended wherever possible.”</p>	<p>States must “ensure” physical security of production locations and materials. The requirement can be met by a “performance based standard approved by DHS”, which must be submitted as part of a State’s mandatory physical security plan. Physical security must include access control, including the use of access badges and “controlled access systems.”</p>
<p>Production Employee Screening</p>	<p>No specific requirement, but member “maintain internal controls to identify and minimize fraud.” Further, each member is required to “establish a formal audit plan and procedures for its driver license and identification processes as a deterrent to internal fraud.”</p>	<p>Background checks are required for all persons who have the ability to enter data, or are involved in the manufacture or production of cards, or who have the ability to affect the identity information on a card, including contractors as well as government employees. Both name based and fingerprint based criminal history checks are required to determine if there is a record that contains specified felonies. In addition, States must conduct financial history checks and lawful status checks through SAVE. States must provide for appeal procedures.</p>

Employee Training	Each jurisdiction must implement a training program for the recognition and detection of fraudulent documents. Program must include the AAMVA fraud recognition materials and guidelines for employees as well as contractors engaged in DL/ID card issuance and must include annual refresher training.	Each State's security plan must include periodic training in "fraudulent document recognition, approved by DHS, for appropriate employees."
Information Sharing	The Driver Control Record (DCR) must be transmitted within thirty(30) days of notice by the new Jurisdiction of Record (JOR). DLA Code convictions must be reported to the JOR within thirty(30) days. The same reporting requirements apply to all Notices of Failure to Comply.	Each State must "provide electronic access to all other States to information contained in the motor vehicle database of the State." According to the NPRM, this must be done in "a manner approved by DHS."
Electronic Communications	Information must be "transmitted by electronic or other means" as maybe "specified in the rules." There is no current express requirement for the means or method of accomplishing electronic communication on a routine basis. Much of the current reporting under the existing compacts is done by paper, mail correspondence.	While the Act mandates mutual electronic exchange, there is no system currently established.

http://www.aamva.org/cgi-bin/MsmGo.exe?grab_id=0&page_id=9946&query=dlc