

REAL ID Final Rules: a Summary

Janice Kephart, President

9/11 Security Solutions LLC

Applicability 37.01

Definitions 37.03

Validity 37.05 and Compliance 37.51 periods

Identity Verification 37.11 and Document Authentication of the Applicant 37.13

 One Driver, One License 37.29

 Source Document Retention 37.31

 DMV Databases 37.33

Hardening the Driver License or ID

 Physical Security Features 37.15

 Surface Requirements 37.17 and Machine Readable Zone 37.19

Categories of Driver License or ID

 Temporary or Limited-Term 37.21

 Reissued 37.23

 Renewal 37.25

 Phase-Ins during Enrollment Period 37.27

 Non REAL ID Driver License or ID 37.71

Security Plan for Employees, Personally Identifiable Information and Production Facilities 37.41-37.45

Procedures for Determining State Compliance 37.59-37.65

Applicability 37.01

REAL ID rules apply to States and U.S. territories that choose to issue drivers' licenses (DLs) that can be accepted by Federal Agencies for 'official purposes', defined as "accessing Federal Facilities, boarding a Federally-Regulated commercial aircraft, and entering nuclear power plants". The Rules also set standards for non-REAL IDs issued in States that are REAL ID compliant.

Definitions 37.03

Lawful Status includes most instances of legal immigration status, including a pending application for asylum.

Personally Identifiable Information means any information that can be used to trace or distinguish identity including Name or SSN (Social Security Number), biometrics such as a photo or signature, or government assigned numbers (such as DL identity number), traceable to an individual.

Material Change is any change to Personally Identifiable Information but does not include change of address of principal residence.

Validity 37.05 and Compliance 37.51 periods

Validity REAL IDs cannot be valid for longer than eight years, but can be valid for a shorter period.

All those born **on or after December 1, 1964** must have REAL ID compliant cards for official purposes **by December 1, 2014**.

All those born **before December 1, 1964** must have REAL ID compliant cards for official purposes **by December 1, 2017**.

After the respective deadlines of 2014 (50 and under) and 2017 (over 50) pass, Federal agencies can no longer accept non-REAL ID compliant driver licenses or Identity Cards (IDs). Non-Compliant Cards issued in States that are REAL ID compliant must clearly indicate on their face and in the MRZ that they are not acceptable for official federal purposes. However, under 37.65(c), if a State is materially compliant and the cards bear a DHS-approved security marking, these cards "will continue to be accepted by federal agencies after the expiration of the enrollment period" described above, "until the expiration date on the face of the document."

Compliance Pursuant to 37.63, if a State requests an extension **by March 31, 2008, DHS may grant an extension to no later than Dec. 31, 2009.** Under 37.51(b), States **must be materially compliant by January 1, 2010 to receive an additional extension towards full compliance by May 11, 2011.** Benchmarks for material compliance (under Appendix A) are as follows:

- (1) **Mandatory facial image capture** and retain such image;
- (2) **Sign declaration** under penalty of perjury **and retain declaration**;
- (3) Require **applicant to present identity source documents** under 37.11(c)(1);
- (4) Require documentation of DOB, SSN, address of principle residence and lawful status;
- (5) Have a documented exceptions process in place;
- (6) Make reasonable efforts to ensure that **applicant does not have more than one DL or ID card under a different identity**;
- (7) **Verify lawful status via SAVE**, the Systematic Alien Verification of Entitlements System;
- (8) **Verify SSN** (Social Security Number) via SSA, (Social Security Administration);
- (9) Issue DLs with **levels 1, 2, and 3 security features** pursuant to 37.15;
- (10) Specified data on face of cards;
- (11) **Mark materially compliant DLs** with a DHS approved security mark;
- (12) **Issue temporary or limited-term licenses** to all individuals with temporary lawful status and match validity of license to end of lawful status. Have a documented security plan in place pursuant to 37.41;
- (13) **Ensure security of personally identifiable information**;
- (14) Require covered employees to attend American Association of Motor Vehicle Administrators (AAMVA) or equivalent fraudulent document recognition training;
- (15) Conduct name and fingerprint based criminal history and employment eligibility checks on all covered employees;

- (16) Commit to material compliance by Jan. 10, 2010 or within 90 days of submission of this document;
- (17) Clearly state on the face of non-compliant DLs or ID that they are not acceptable for official federal purposes

Under [37.51\(a\)](#) States must be fully compliant (a total of 39 benchmarks) by May 11, 2011. To meet this deadline, states must file a State certification from the highest executive overseeing the DMV in the State, with a letter from the State Attorney General confirming legal authority to impose rules, a Security Plan (see [37.41](#)), and exceptions process by Feb. 11, 2011, see [37.55](#).

Identity Verification 37.11 and Document Authentication of the Applicant 37.13

The Applicant must provide sufficient documentation for a state to both verify identity and authenticate documents presented for the purpose of establishing identity. States may choose to have a documented exceptions process for individuals who are unable to present all documents and must rely on alternate documents. Alternate documents to prove lawful status may only be used by U.S. Citizens. States are not required to comply with these requirements when issuing DLs or IDs in support of ‘Federal, State, or local criminal justice agencies’ who require special licensing for individuals on official duty, or for ‘safeguarded persons’.

Identity is established by a combination of biometric (digital photo only) and verified government-issued identity documents. Under [37.13](#), “States shall use systems for electronic verification of document and identity data as they become available.” If information about identity does not verify, a state may issue a non-compliant DL or ID while awaiting a non-match resolution.

Applicants must provide the following to establish identity:

Facial image capture prior to DL/ID issuance, maintained by the state for 5 years if no card is issued, 2 years beyond its expiration if it is .

Declaration under penalty of perjury that information provided is true and correct, maintained by state.

Identity and lawful status can be verified with any of the following documents:

Valid unexpired passport

Certified birth record showing US citizenship

Consular Report of Birth Abroad

Note: State Department issued documents do not yet have a means of verification with DHS.

DHS Certificates of Naturalization or Citizenship

Valid, unexpired permanent resident card

Identity, but not proof of lawful status, can be verified as follows:

Valid, unexpired employment authorization document

Valid, unexpired foreign passport with valid visa with most recent US admittance

Note: **lawful status** must be authenticated by one check in SAVE. If there is a non-match, DMV cannot issue a REAL ID and until there is resolution with the US Citizenship and Immigration Services for resolution. 37.13(b)(1)

DOB, can be verified with any of the listed documents that also verify Identity. Birth certificates should be verified through the Electronic Verification of Vital Events (EVVE) system or other DHS-approved method. If documents do not appear authentic or there is a non-match, no DL/ID shall be issued until there is resolution with the issuing office. 37.13(b)(3)

Social security card, W-2, 1099 form or other similar documents checked against the SSOLV (SSN match) database. If there is a non-match, DMV cannot issue a REAL ID and until the information is verified the SSA. 37.13(b)(2)

Principal Residence Demonstrated with two documents of state's choosing showing both name and address. (Exceptions, usually for safety or protection, exist).

One Driver, One License 37.29 States must make 'reasonable efforts' to ensure that the applicant does not hold multiple DLS or IDs in that state or any other states under different identities or names. If other DLs or IDs are found, the state of application must ensure that other DLs or IDs have been terminated prior to issuing a new REAL ID DL or ID by verification with the issuing state. 37.13(b)(6).

Source Document Retention 37.31 All applications, declarations and source documents obtained under 37.11 shall be protected, see 37.41(b)(2). Paper copies must be retained for 7 years minimum, digital and microfiche images for 10 years minimum.

The only exception is birth certificates, where the applicant can request that the actual certificate image not be stored, but only the relevant data contained on the certificate.

Photo images must be stored as JPEGs in a manner that is interoperable with other States' photo capture. A similar requirement is imposed for maintenance of document and signature images.

All images must be retrievable by the DMV for law enforcement use.

DMV Databases 37.33 All DMV databases must contain the following minimum information: all information that appears on the driver's license or ID, including untruncated full legal name, all MRZ data; motor vehicle driver histories including points, violations and suspensions.

Hardening the Driver License or ID

Physical security features 37.15(a) and (b) A key feature of REAL ID is that the cards include "document security features on REAL ID drivers' licenses and identification cards designed to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards in accordance with this section." Technologies must not be commonly available to the general public, multi-layered, and able to be integrated into the cards.

37.15(c) Three levels of security are required to detect false cards.

Level 1 requires that an 'easily identifiable visual or tactile feature' for cursory examination without any aids.

Level 2 is a feature detected by 'trained inspectors with simple equipment'.

Level 3 is a feature only detectable by forensic inspectors.

37.15(d) Once States complete such a card design, they must certify that the design meets DHS requirements and submit a report indicating the card's ability to deter and detect forgery and counterfeiting. DHS reserves the right to require independent forensic analysis of the card.

Surface Requirements 37.17 and **Machine Readable Zone 37.19** (Items in green are also required to be data elements in the MRZ.)

Full legal name, same as the source document, unless State law or regulation allows otherwise; **DOB**; **Gender**; **unique driver license or ID number** (not SSN);

full facial digital photo per ICAO standards; **address of principal residence** but not those in a State or Federal confidentiality program (e.g. domestic violence or sexual crimes), or court order, or otherwise by law; signature as required by the AAMVA 2005 standard; physical security features; **date of transaction**; expiration date; state/territory of issuance; and all printed information must be to ICAO standards. *The MRZ must also contain the **State's card design revision date and inventory control number**, neither of which is required on the surface of the document. The MRZ must use the PDF417 2D standard, the most recent in barcode technologies maximizing data storage in the smallest space.*

37.17(n) All cards shall bear a **DHS-approved security marking** reflecting whether the card is materially or fully compliant with these Rules.

Categories of Driver License or ID

REAL ID sets standards for the varieties of cards a State can issue.

Temporary or Limited-Term 37.21 These cards are for those who have temporary lawful status in the U.S., and must be clearly marked as such. The key here is that these cards cannot be issued for a time longer than the applicant's authorized stay by immigration authorities. If there is no expiration date for lawful status, the DL/ID cannot be valid for longer than one year. Each reauthorization must be submitted through SAVE for verification of status.

Reissued 37.23 States must set forth procedures to verify identity for the purposes of reissuance so that the same individual as originally applied is reissued. Remote (non-in-person) reissuance is permissible, as long as the applicant's SSN and lawful status is re-verified first and there has been no material change to any personally identifiable information (does not include residence information). Any material change requires verification via 37.13.

Renewal 37.25 In person renewals must occur no less frequently than every 16 years, take an updated digital image, re-verify SSN and lawful status, and any other original documentation it was not able to because issuance systems or processes did not exist (such as State Department documentation verification).

Non REAL ID Driver License or ID 37.71 States are free to issue non REAL IDs along with REAL IDs by law as long such drivers' licenses or IDs(1) Clearly state on their face on the MRZ that the DL/ID is not acceptable for official purposes

Security Plan for Employees, Personally Identifiable Information and Production Facilities 37.41-37.45

As part of its certification, States must submit a security plan that contains the following elements:

- (1) **37.41(b)(1) Physical security** of production facilities and storage areas for card stock and production.
- (2) **37.41(b)(2) Security of personally identifiable information** as follows: All documents presented to show identity and lawful status or other personally identifiable information shall be protected as described in their security plan including (1) procedures to prevent “unauthorized access, use, or dissemination of applicant information and images of source documents” retained under REAL ID and “standards and procedures for document retention and destruction; (2) a privacy policy; (3) and compliance with the Driver’s Privacy Protection Act, 18 USC § 2721.
- (3) **37.41(b)(3) Document and Physical Security Features of the Card** and the State’s use of biometrics
- (4) **37.41(b)(4) and (5) Employee access control** including credentialing; background checks; access to systems; **fraudulent document training** and security awareness training. Under **37.45**, background checks for employees include prior employment references, named and fingerprint based criminal history checks and employment eligibility verification. The States is “encouraged to participate in the USCIS E-Verify program.
- (5) **37.41(b)(8)** A separate report on how a State will safeguard identities as necessary in coordination with government and law enforcement entities.

Procedures for Determining State Compliance 37.51-37.65

States are subject to DHS audits to determine compliance, including onsite inspections and interviews of employees. Audits must be conducted within 45 days of DHS receiving a State’s certification of material or full compliance.

If DHS determines material compliance is met, DHS may grant an extension until May 10, 2011 for full compliance.

If DHS does not determine material compliance has been met, the State has 30 days to respond or explain corrective action it intends to take. DHS then has another 45 days to make a final determination.

A State can fail to comply with REAL ID by (1) failing to submit a certification or (2) failing to meet one or more of the standards in the Rule.