

prior issuance. All material changes must be established through the applicant's presentation of an original source document as provided in Subpart B, and must be verified as specified in § 37.13.

§ 37.27 Driver's licenses and identification cards issued during the age-based enrollment period.

Driver's licenses and identification cards issued to individuals prior to a DHS determination that the State is materially compliant may be renewed or reissued pursuant to current State practices, and will be accepted for official purposes until the validity dates described in § 37.5. Effective December 1, 2014, Federal agencies will only accept REAL ID cards for official purpose from individuals under 50 as of December 1, 2014. Individuals age 50 or older on December 1, 2014, must obtain and present REAL ID cards for official purposes by December 1, 2017.

§ 37.29 Prohibition against holding more than one REAL ID card or more than one driver's license.

(a) An individual may hold only one REAL ID card. An individual cannot hold a REAL ID driver's license and a REAL ID identification card simultaneously. Nothing shall preclude an individual from holding a REAL ID card and a non-REAL ID card unless prohibited by his or her State.

(b) Prior to issuing a REAL ID driver's license,

(1) A State must check with all other States to determine if the applicant currently holds a driver's license or REAL ID identification card in another State.

(2) If the State receives confirmation that the individual holds a driver's license in another State, or possesses a REAL ID identification card in another State, the receiving State must take measures to confirm that the person has terminated or is terminating the driver's license or REAL ID identification card issued by the prior State pursuant to State law, regulation or procedure.

(c) Prior to issuing a REAL ID identification card,

(1) A State must check with all other States to determine if the applicant

currently holds a REAL ID driver's license or identification card in another State.

(2) If the State receives confirmation that the individual holds a REAL ID card in another State the receiving State must take measures to confirm that the person has terminated or is terminating the REAL ID driver's license or identification card issued by the prior State pursuant to State law, regulation or procedure.

Subpart C—Other Requirements

§ 37.31 Source document retention.

(a) States must retain copies of the application, declaration and source documents presented under § 37.11 of this Part, including documents used to establish all names recorded by the DMV under § 37.11(c)(2). States shall take measures to protect any personally identifiable information collected pursuant to the REAL ID Act as described in their security plan under § 37.41(b)(2).

(1) States that choose to keep paper copies of source documents must retain the copies for a minimum of seven years.

(2) States that choose to transfer information from paper copies to microfiche must retain the microfiche for a minimum of ten years.

(3) States that choose to keep digital images of source documents must retain the images for a minimum of ten years.

(4) States are not required to retain the declaration with application and source documents, but must retain the declaration consistent with applicable State document retention requirements and retention periods.

(b) States using digital imaging to retain source documents must store the images as follows:

(1) Photo images must be stored in the Joint Photographic Experts Group (JPEG) 2000 standard for image compression, or a standard that is interoperable with the JPEG standard. Images must be stored in an open (consensus) format, without proprietary wrappers, to ensure States can effectively use the image captures of other States as needed.

(2) Document and signature images must be stored in a compressed Tagged Image Format (TIF), or a standard that is interoperable with the TIF standard.

(3) All images must be retrievable by the DMV if properly requested by law enforcement.

(c) Upon request by an applicant, a State shall record and retain the applicant's name, date of birth, certificate numbers, date filed, and issuing agency in lieu of an image or copy of the applicant's birth certificate, where such procedures are required by State law.

§ 37.33 DMV databases.

(a) States must maintain a State motor vehicle database that contains, at a minimum—

(1) All data fields printed on driver's licenses and identification cards issued by the State, individual serial numbers of the card, and SSN;

(2) A record of the full legal name and recorded name established under § 37.11(c)(2) as applicable, without truncation;

(3) All additional data fields included in the MRZ but not printed on the driver's license or identification card; and

(4) Motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on driver's licenses.

(b) States must protect the security of personally identifiable information, collected pursuant to the REAL ID Act, in accordance with § 37.41(b)(2) of this part.

Subpart D—Security at DMVs and Driver's License and Identification Card Production Facilities

§ 37.41 Security plan.

(a) *In General.* States must have a security plan that addresses the provisions in paragraph (b) of this section and must submit the security plan as part of its REAL ID certification under § 37.55.

(b) Security plan contents. At a minimum, the security plan must address—

(1) Physical security for the following:

(i) Facilities used to produce driver's licenses and identification cards.

(ii) Storage areas for card stock and other materials used in card production.

(2) Security of personally identifiable information maintained at DMV locations involved in the enrollment, issuance, manufacture and/or production of cards issued under the REAL ID Act, including, but not limited to, providing the following protections:

(i) Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act. These safeguards must include procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction.

(ii) A privacy policy regarding the personally identifiable information collected and maintained by the DMV pursuant to the REAL ID Act.

(iii) Any release or use of personal information collected and maintained by the DMV pursuant to the REAL ID Act must comply with the requirements of the Driver's Privacy Protection Act, 18 U.S.C. 2721 *et seq.* State plans may go beyond these minimum privacy requirements to provide greater protection, and such protections are not subject to review by DHS for purposes of determining compliance with this Part.

(3) Document and physical security features for the card, consistent with the requirements of § 37.15, including a description of the State's use of biometrics, and the technical standard utilized, if any;

(4) Access control, including the following:

(i) Employee identification and credentialing, including access badges.

(ii) Employee background checks, in accordance with § 37.45 of this part.

(iii) Controlled access systems.

(5) Periodic training requirements in—