

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—

(i) Fraudulent document recognition training for all covered employees handling source documents or engaged in the issuance of driver's licenses and identification cards. The fraudulent document training program approved by AAMVA or other DHS approved method satisfies the requirement of this subsection.

(ii) Security awareness training, including threat identification and handling of SSI as necessary.

(6) Emergency/incident response plan;

(7) Internal audit controls;