(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—

(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;

(8) An affirmation that the State possesses both the authority and the means to produce, revise, expunge, and protect the confidentiality of REAL ID driver's licenses or identification cards issued in support of Federal, State, or local criminal justice agencies or similar programs that require special licensing or identification to safeguard persons or support their official duties. These procedures must be designed in coordination with the key requesting authorities to ensure that the procedures are effective and to prevent conflicting or inconsistent requests. In order to safeguard the identities of individuals, these procedures should not be discussed in the plan and States should make every effort to prevent disclosure to those without a need to know about either this confidential procedure or any substantive information that may compromise the confidentiality of these operations. The appropriate law enforcement official and United States Attorney should be notified of any action seeking information that could compromise Federal law enforcement interests.

(c) *Handling of Security Plan*. The Security Plan required by this section contains Sensitive Security Information (SSI) and must be handled and protected in accordance with 49 CFR part 1520.

§ 37.43 Physical security of DMV production facilities.

(a) States must ensure the physical security of facilities where driver's licenses and identification cards are produced, and the security of document materials and papers from which driver's licenses and identification cards are produced or manufactured.

(b) States must describe the security of DMV facilities as part of their security plan, in accordance with § 37.41.

§ 37.45 Background checks for covered employees.

(a) *Scope*. States are required to subject persons who are involved in the manufacture or production of REAL ID driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card, or current employees who will be assigned to such positions (''covered employees'' or ''covered positions''), to a background check. The background check must include, at a minimum, the validation of references from prior employment, a name-based and fingerprint-based criminal history records check, and employment eligibility verification otherwise required by law. States shall describe their background check process as part of their security plan, in accordance with § 37.41(b)(4)(ii). This section also applies to contractors utilized in covered positions.

(b) *Background checks*. States must ensure that any covered employee under paragraph (a) of this section is provided notice that he or she must undergo a background check and the contents of that check.

(1) *Criminal history records check*. States must conduct a name-based and fingerprint-based criminal history records check (CHRC) using, at a minimum, the FBI's National Crime Information Center (NCIC) and the Integrated Automated Fingerprint Identification (IAFIS) database and State repository records on each covered employee identified in paragraph (a) of this section, and determine if the covered employee has been convicted of any of the following disqualifying crimes:

(i) *Permanent disqualifying criminal offenses*. A covered employee has a permanent disqualifying offense if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction, of any of the felonies set forth in 49 CFR 1572.103(a).

(ii) *Interim disqualifying criminal offenses*. The criminal offenses referenced in 49 CFR 1572.103(b) are disqualifying