DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 37

[Docket No. DHS–2006–0030]

RIN 1601–AA37

Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes

AGENCY: Office of the Secretary, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is proposing to establish minimum standards for State-issued driver's licenses and identification cards that Federal agencies would accept for official purposes after May 11, 2008, in accordance with the REAL ID Act of 2005. This rule proposes standards to meet the minimum requirements of the REAL ID Act of 2005, including: information and security features that must be incorporated into each card; application information to establish the identity and immigration status of an applicant before a card can be issued; and physical security standards for locations where driver's licenses and applicable identification cards are issued.

DATES: Submit comments by May 8, 2007.

ADDRESSES: You may submit comments, identified by the DHS docket number DHS–2006–0030 that corresponds to this rulemaking, using any one of the following methods:

- Federal Rulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Fax: 866–466–5370.
- Mail: Paper, disk or CD–ROM submissions can be mailed to the Department of Homeland Security, Attn: NAC 1–12037, Washington, DC 20528.

FOR FURTHER INFORMATION CONTACT: Darrell Williams, REAL ID Program Office, Department of Homeland Security, Washington, DC 20528 (202) 282–9829.

SUPPLEMENTARY INFORMATION:

Public Participation

The Department of Homeland Security (DHS) invites interested persons to participate in this rulemaking by submitting written comments or data, and has requested comments on specific portions of this rulemaking as described in section VI below. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. See **ADDRESSES** above for information on where to submit comments.

With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. The most helpful comments reference a specific portion of the rulemaking, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, by fax, or by mail as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail, submit them in two copies, in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you want DHS to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it back to you.

DHS will file in the public docket all comments received by DHS, except for comments containing confidential information and sensitive security information (SSI).[1] DHS will consider all comments received on or before the closing date for comments. The docket is available for public inspection.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in the **FOR FURTHER INFORMATION CONTACT** section.

Upon receipt of such comments, DHS will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. DHS will hold them in a separate file to which the public does not have access, and place a note in the public docket that DHS has received such materials from the commenter. If DHS receives a request to examine or copy this information, DHS will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's (DHS') FOIA regulations found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published at www.regulations.gov. You may also review the comments in the public docket on the Internet at *http://www.regulations.gov.*

Availability of Rulemaking Document

You can get an electronic copy using the Internet by—

(1) Searching on www.regulations.gov by docket number or title, or

(2) Accessing the Government Printing Office's Web page at *http://www.gpoaccess.gov/fr/index.html.*

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Abbreviations and Terms Used in This Document

AAMVA—American Association of Motor Vehicle Administrators
CAC—Department of Defense Common Access Card
CBP—Customs and Border Protection
CDLIS—Commercial Driver's License Information System
CHRC—Criminal History Records Check
CRBA—Consular Report of Birth Abroad
DHS—Department of Homeland Security
DMV—Department of Motor Vehicles
DOS—Department of State
DOT—Department of Transportation
EAD—Employment Authorization Document
EVVE—Electronic Verification of Vital Events
HHS—Department of Health and Human Services
IAFIS—Integrated Automated Fingerprint Identification
ICAO—International Civil Aviation Organization
ID—Identification Card
LPR—Lawful Permanent Resident
MRT—Machine Readable Technology

[1] ''Sensitive Security Information'' or ''SSI'' is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

MRZ—Machine Readable Zone
NCSL—National Conference of State Legislatures
NCIC—National Crime Information Center
NGA—National Governors Association
NPRM—Notice of Proposed Rulemaking
PDPS—Problem Driver Pointer System
SAVE—Systematic Alien Verification for Entitlements
SEVIS—Student and Exchange Visitor Information System
SSA—Social Security Administration
SSI—Sensitive Security Information
SSN—Social Security Number
SSOLV—Social Security On-Line Verification
TIF—Tagged Image Format
TSA—Transportation Security Administration
TWIC—Transportation Worker Identification Credential
USCIS—U.S. Citizenship and Immigration Services
VWP—Visa Waiver Program
WHTI—Western Hemisphere Travel Initiative

Table of Contents

I. Background

A. Statutory Authority

The REAL ID Act of 2005 [2] (the Act) prohibits Federal agencies, effective May 11, 2008, from accepting a driver's license or DMV-issued personal identification card issued by a State for an official purpose unless the issuing State is meeting the requirements of the Act. The Act requires DHS to determine whether a State is meeting the Act's requirements based upon certifications submitted by each State in a manner prescribed by DHS. The Secretary of Homeland Security is authorized under section 203 of the Act to issue regulations as necessary to set the standards required under the Act. This rule proposes implementation standards for States to meet the Act's requirements for issuance of driver's licenses and identification cards intended for acceptance by Federal agencies for official purposes.

The Act sets forth minimum document requirements, minimum driver's license and identification card issuance standards, and other requirements, including the following—

- Information and features that must appear on the face of the driver's license or identification card, and inclusion of a common machine-readable portion of a driver's license or identification card;
- Presentation and verification of information an applicant must provide before a driver's license or identification card may be issued, including evidence that the applicant is a U.S. citizen or has lawful status in the United States;
- Physical security of locations where driver's licenses and identification cards are produced, the security of document materials and papers from which driver's licenses and identification cards are produced, and the background check of certain employees involved in the manufacture and production of licenses, and;
- Physical security of the driver's licenses and identification cards to prevent tampering, counterfeiting, and duplication of the documents for a fraudulent purpose.

The Act also permits a State otherwise in compliance with the Act to issue driver's licenses and identification cards that do not conform to the Act's requirements. Such driver's licenses and identification cards, however, cannot be used for an official purpose and must clearly state on the face of the card that a Federal agency may not use it for an official purpose. The State also must use a unique design or color indicator so that it is readily apparent to Federal agency personnel that the card is not to be accepted for an official purpose.

Section 203 of the Act amends 18 U.S.C. 1028(a) to establish a Federal criminal penalty for persons who knowingly traffic in actual authentication features for use in fraudulent identification cards.

B. Consultation With the States, Non-Governmental Organizations, and the Department of Transportation

Section 205(a) of the Act requires that any regulations, standards, or grants under the Act be carried out in consultation with the Secretary of Transportation and the States. DHS has met and consulted with the Department of Transportation (DOT), and formed an interagency work group to develop these proposed regulations. DOT and other Federal agencies with an interest in this rulemaking participated actively in the work group.

DHS has also consulted with State officials and State representative associations in the development of this proposed rule through meetings and conference calls in 2005 and 2006. Many States and State representative associations participated in these events and submitted written comments for consideration in the development of this proposed rule. These are available for inspection in the public docket.

In particular, DHS received comments from the National Governors

[2] Division B—REAL ID Act of 2005, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109–13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note).

Association (NGA), the National Conference of State Legislatures (NCSL), and the American Association of Motor Vehicle Administrators (AAMVA), which aggregated responses from 48 jurisdictions impacted by REAL ID, including 46 States, American Samoa, and the District of Columbia. DHS also met with various non-governmental organizations (NGOs), particularly civil rights, privacy and religious groups. The States and NGOs raised a series of concerns about the requirements mandated under the Act. A summary of these concerns is outlined below. DHS addresses each of these concerns in the discussion of the proposed requirements under this rule in section II.

One of the first issues of concern to the States was the brief period for compliance. There was concern that DHS would interpret the Act in such a way as to require that all driver's licenses and identification cards nationally be brought into compliance with the Act by May 2008, an impossible task according to the States. The States instead suggested a ''date forward'' approach, which we have proposed to adopt as a phase-in period through May 2013.

The detailed requirements of the Act, particularly requirements for original documents and proof of principal residence, also raised State concerns that individuals, through no fault of their own, might not be able to meet certain requirements of the Act. The States advocated for an exceptions process to accommodate certain circumstances (victims of natural disasters such as Hurricanes Katrina and Rita who no longer have certain documents, or elderly individuals with no birth certificate, for example). We understand these concerns and therefore propose that the States adopt an exceptions process in their Departments of Motor Vehicles (DMVs) that will be monitored by the State and included as part of the State's certification process to DHS. This exception process would include any difficulties arising from attempts to verify birth information for individuals born before 1935, who, due to various considerations, may not have been issued birth certificates.

The Act requires States to subject certain individuals involved in the manufacture and production of driver's licenses and identification cards to appropriate background checks. The States have suggested to DHS that, due to the unique structure of each State's DMV system, the identification of positions that should be subject to this requirement be left up to the States. DHS agrees with this proposal. The States have also proposed that new hires be allowed to begin work at the DMVs while their background check is pending. DHS understands that the States must have flexibility in their hiring, and therefore proposes that States place new employees in positions that are not subject to the background check until the check is complete and satisfaction of employment conditions for the covered position is determined.

The States have indicated to DHS that the Act will lead to an increase in the number of required in-person visits to DMVs. Generally speaking, the States have sought to utilize alternate service channels (particularly the internet and services by mail) to reduce the required number of in-person visits to DMVs, as a means of reducing State costs and improving service to customers. The States have, therefore, expressed particular concerns with the renewal process under REAL ID. DHS understands these concerns and is therefore proposing that States continue their remote renewal procedures, as long as they establish a procedure to verify the identity of individuals applying for renewal remotely, maintain images of the source documents the individual used to obtain a REAL ID driver's license or identification card, and establish a procedure to re-verify the information on the source documents retained by the State. DHS proposes, however, that individuals with temporary REAL ID driver's licenses or temporary identification cards renew their documents in person, in order to present evidence of continued lawful status.

C. Summary of the Proposed Rule

DHS proposes to issue REAL ID regulations that create minimum standards for State driver's licenses and identification cards that Federal agencies can accept for official purposes on or after May 11, 2008. Under this proposal, States must certify that they are in compliance with these requirements, and DHS must concur, before the driver's licenses and identification cards that the States issue may be accepted by Federal agencies for official purposes on or after May 11, 2008. Because DHS recognizes that not all driver's licenses and identification cards can be reissued by May 11, 2008, the proposal provides a five-year phase-in period for driver's license or identification card renewals. All driver's licenses and identification cards that are intended to be accepted for official purposes as defined in these regulations must be REAL ID licenses and identification cards by May 11, 2013

Key features of the proposal include:

- *Applicant documentation.* States would require individuals obtaining driver's licenses or personal identification cards to present documentation to establish identity; U.S. citizenship or lawful immigration status as defined by the Act; date of birth; social security number (SSN) or ineligibility for SSN; and principal residence. States may establish an exceptions process for the documentation requirement, provided that each such exception is fully detailed in the applicant's motor vehicle record.
- *Verification requirements.* States would verify the issuance, validity, and completeness of a document presented. This proposal specifies electronic verification methods depending on the category of the documents.
- *Information on driver's licenses and identification cards.* The following information would be required to appear on State-issued driver's licenses and identification cards: full legal name, date of birth, gender, a unique driver's license or identification card number (not the SSN), a full facial digital photograph, address of principal residence (with certain exceptions), issue and expiration dates, signature, physical security features and a common machine-readable technology (MRT).
- *Security features on the card.* The proposal contains standards for physical security features on the card designed to prevent tampering, counterfeiting or duplication for a fraudulent purpose, and a common MRT with defined data elements.
- *Physical security/security plans.* Each State must prepare a comprehensive security plan for all State DMV offices and driver's license/identification card storage and production facilities, databases and systems and submit these plans to DHS as part of its certification package.
- *Employee background checks.* States would conduct name-based and fingerprint-based criminal history records checks against State criminal records and the FBI's NCIC and IAFIS, respectively, on certain employees working in State DMVs who have the ability to affect the identity information that appears on the driver's license or identification card, who have access to the production process, or who are involved in the manufacture of the driver's licenses and identification cards. States would pay a fee to FBI to cover the cost of this check. States would also conduct a financial history check on these employees.
- *State certification process.* Similar to DOT regulations governing State

administration of commercial driver's licenses (49 CFR part 383), States will be required to submit a certification and specified documents to DHS to demonstrate compliance with these regulations and demonstrate continued compliance annually.

• *Database connectivity.* States would be required to provide electronic access to specific information contained in the motor vehicle database of the State to all other States.

II. Analysis of This Proposed Rule

A. Scope and Applicability

The Act does not require any State to issue REAL ID driver's licenses and identification cards. States may choose to issue driver's licenses and identification cards that cannot be accepted by Federal agencies for official purposes (referred to in this document as ''non-REAL ID driver's licenses and identification cards''). This proposed rule would apply to States and territories that choose to issue driver's licenses and identification cards that Federal agencies can accept for official purposes. Consistent with section 202(d)(11) of the Act, this rule also proposes requirements for issuance of non-REAL ID driver's licenses (as well as non-REAL ID identification cards) by States in compliance with the Act. Under this proposed rule, individuals can hold only one valid REAL ID driver's license or identification card at a time.

DHS understands that at present an individual may hold active driver's licenses in multiple jurisdictions. Although DHS is not regulating issuance of non-REAL ID driver's licenses beyond what is required in the REAL ID Act, DHS wishes to further the concept of ''one driver, one record, one record of jurisdiction'' and seeks comment on how the REAL ID Act may be implemented to discourage the issuance of multiple non-REAL ID driver's licenses to an individual, or what steps States can take to ensure individuals are not holding multiple driver's licenses from multiple States.

1. Definition of ''Official Purpose''

Section 201(3) of the Act provides that the term ''official purpose'' ''includes but is not limited to accessing Federal facilities, boarding Federally-regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.'' DHS proposes to limit the regulatory definition of ''official purpose'' at this time, to those purposes expressly stated in the Act—accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants. DHS, under the discretionary authority granted to the Secretary of Homeland Security under the Act, may expand this definition in the future. DHS seeks comment on the proposed scope of ''official purpose,'' and how DHS could expand this definition to other federal activities.

DHS considered including the acquisition of Federally-issued identification documents, such as a Transportation Worker Identification Card (TWIC), military Common Access Card (CAC), passport, or PASSport card within the proposed definition of ''official purpose.'' To do so would be consistent with the concept of strengthening the reliability of identity documents, one of the primary objectives of the Act. However, since no State would be required to have all of its citizens possess Real ID driver's licenses and identification cards until May 2013, DHS concluded that it would be premature to require Federal agencies to accept only Real ID driver's licenses and identification cards during the phase-in period and that the imposition of such a requirement could inhibit individuals from obtaining these necessary forms of Federal identification.

Federal agencies themselves do not currently examine identification from all individuals seeking to board regulated commercial aircraft or to enter nuclear power plants. In the case of aircraft, often it is aircraft operators that examine driver's licenses or other identification credentials of individuals seeking entry to the sterile area of an airport. However, they do so in compliance with requirements in security programs issued pursuant to TSA regulations. DHS interprets the language of the REAL ID statute to mean that when nongovernmental entities require identification for the scope of activities considered ''official purposes'' in compliance with Federal requirements, and an individual presents a driver's license or DMV-issued identification card, the REAL ID Act's federal acceptance requirements would also apply to these nongovernmental entities.

These regulations are not intended to change current admittance practices at Federal facilities. If a Federal facility does not currently require presentation of photo identification prior to entry, the Act and these proposed regulations would not require that process to change. Similarly, if a Federal facility currently accepts identification other than a State-issued driver's license or identification card, the Act and these proposed regulations do not require that the agency refuse to accept such other forms of identification. If the individual intends to use a State-issued driver's license or identification card, however, it must be one that is issued by a State that is complying with the REAL ID Act.

2. Definition of ''REAL ID Driver's License or Identification Card''

Throughout this proposed rule, driver's licenses and identification cards issued under these regulations that Federal agencies may accept for official purposes are referred to as ''REAL ID driver's licenses and identification cards.'' The term ''REAL ID driver's licenses and identification cards'' includes driver's licenses and identification cards issued by State DMVs (or other State agencies with comparable responsibility for issuing driver's licenses and identification cards) to U.S. citizens and Lawful Permanent Residents (LPRs) of the United States for a maximum renewable period of eight years. The term ''REAL ID driver's licenses and identification cards'' also includes driver's licenses and identification cards acceptable for official purposes that are issued to aliens legally present in the United States for a finite period of time, upon verification of their current lawful status for the period of their authorized length of stay, or for one year, if no length of stay is specified. In instances where the proposed regulation discusses these temporary driver's licenses and identification cards independently, these types of REAL ID licenses and identification cards are referred to as ''temporary REAL ID driver's licenses and identification cards.''

3. Definition of ''Identification Card''

Section 201(2) of the Act defines ''identification card'' to mean ''a personal identification card, as defined in section 1028(d) of title 18 United States Code, issued by a State.'' In turn, 18 U.S.C. 1028(d) defines this term, in pertinent part, to mean ''a document made or issued by or under the authority of * * * a State [or] a political subdivision of a State * * * which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals[.]'' Section 201(2), by its express terms, could cover any identification card issued by or under the authority of a State, including identification cards for State-chartered universities and colleges, and cards issued by State agencies to obtain public benefits. At this time, DHS is limiting the scope of this definition to identification cards issued by State

DMVs or other State offices with comparable responsibility for issuing driver's licenses.

DHS believes that these additional documents mentioned above are not currently accepted as identification documents to the same degree as State-issued driver's licenses and identification cards issued by a State DMV. In addition, it would be unduly burdensome at this time for DHS to require that the issuers of these additional documents comply with these proposed standards, since DMVs have been considering the Act's requirements for some time, and it is likely that universities and other State entities have not.

B. Compliance Period

Section 202(a)(3) of the Act provides that, ''[b]eginning 3 years after the date of enactment of this division, a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements of this section.'' The Act further states that DHS ''shall determine whether a State is meeting the requirements of [the Act] based on certifications made by the State to the Secretary.'' *Id.,* (a)(2). DHS, the Department charged with implementing and enforcing the REAL ID Act requirements for identification standards, interprets the compliance provision to mean that effective on May 11, 2008, Federal officials will be prohibited from accepting State-issued driver's licenses and identification cards for official purpose unless the State has submitted the required certification or extension application to DHS and DHS has determined that the State is meeting the requirements of the Act. DHS is proposing under this rule to find that a State certification is sufficient for compliance under the Act if the State has established a program that ensures the State's DMVs will begin issuing driver's licenses and identification cards that meet the requirements of the Act and standards proposed under this regulation beginning May 11, 2008. DHS does not interpret the Act as requiring the States to recall and reissue all driver's licenses and identification cards by May 11, 2008. Rather, States will be able to replace all driver's licenses and identification cards with REAL ID driver's licenses and identification cards intended to be accepted for official purposes by May 11, 2013.

Accordingly, DHS proposes the following compliance requirements:

(1) Each State must submit its certification package to DHS on its REAL ID driver's license and identification card programs no later than February 10, 2008, 90 days before the May 11, 2008 compliance date required under the Act. DHS strongly encourages States to communicate their intent to certify compliance or request an extension by October 1, 2007;

(2) DHS will not find that a State is meeting the requirements of the Act if the State's certification does not demonstrate that the all REAL ID driver's licenses and identification cards issued by the State on or after May 11, 2008, will meet the standards required under the Act and proposed under these regulations, unless the State has sought and received an extension;

(3) For unexpired driver's licenses and identification cards issued prior to May 11, 2008, DHS proposes a five-year phase-in period to allow individuals to apply for and receive new driver's licenses and identification cards that comply with these rules. These driver's licenses and identification cards would be acceptable for official purposes until they expire, or until the phase-in period ends, on May 10, 2013—whichever is earlier. Driver's licenses and identification cards issued before May 11, 2008 that do not expire until after the phase-in period ends would have to be exchanged for driver's licenses and identification cards issued under the new rules in order to be accepted by Federal agencies for official purposes after May 10, 2013.

If a driver's license or identification card that would not otherwise expire until after May 11, 2008 needs to be reissued by a State prior to its expiration date, DHS is proposing that the driver's license or identification card must meet the new standards at the time it is reissued. This reissuance would occur, for example, if a driver's license or identification card has been lost or stolen and needs to be replaced, or if changes in information occur which would cause the DMV to issue a new driver's license or identification card.

Under section 205(b) of the Act, DHS may grant an extension of time to meet the requirements of the Act if the State provides adequate justification. DHS recognizes that many States need a final rule in order to guide their implementation efforts. Many States have informed DHS that, absent sufficient time to consider and act upon the final rule, the States will not be in a position to comply with the Act and the final rule. In recognition of this fact, DHS is establishing a mechanism where States can request an expedited extension of the compliance deadline. States may request an extension based on the lack of a final REAL ID rule by filing such a request no later than October 1, 2007. Based on information already received by DHS, and absent extraordinary circumstances, an extension request will be deemed justified for a period lasting until, but not beyond, December 31, 2009.

Under this provision of the Act, DHS also intends to issue compliance guidance to the States. This guidance will set forth benchmarks or best practices against which progress toward full compliance will be measured and to assist States in drafting the certification packages. As proposed in this rule, DHS would require submission of certifications no later than February 10, 2008, but the Department strongly encourages States to submit certification packages by October 1, 2007. State certification packages should include milestones, schedules, and estimated resources needed to meet all the requirements of the final rule no later than May 11, 2008. States will resubmit and DHS will re-evaluate State plans on an annual basis until all requirements of this rule are met. DHS welcomes comments from the States on appropriate benchmarks for measuring progress toward meeting the requirements of this rule and on specific resource and schedule constraints in meeting these benchmarks.

C. Privacy Considerations

The public has long been accustomed to providing personal information for the purpose of obtaining driver's licenses and identification cards and to having this information printed on driver's licenses. Most States already include this information in a machine readable technology (MRT). With the enactment of the REAL ID Act, however, there has been increased attention to the privacy ramifications involving the information that will appear on the licenses and identification cards and the exchange of information. Some have raised concerns that the Act could create an increased risk of identity theft and erode privacy, or be a stepping-stone to a national identity card.

A frequently-heard concern relates to the amount of additional information the Federal Government will have about driver's license holders and what the Federal Government will do with that data. In fact, however, neither the Real ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before. Moreover, there is no information about a licensee that the Federal Government will store that it is not already required to store.

As described below, DHS has sought to address these privacy concerns within the limits of its authority under

the Act.[3] At the Federal level, only the Driver's Privacy Protection Act of 1994 (DPPA)[4] addresses the privacy of motor vehicle records, but its protections are limited. Although it addresses the use and disclosure of personal information stored in State motor vehicle records, the DPPA does not provides privacy protections for the personal information stored on the licenses themselves or set any security requirements for the motor vehicle databases. DHS has sought in the NPRM to provide for appropriate privacy and security protections to the extent of its authority.

This section of the NPRM will summarize the requirements of the Act that potentially have the greatest impact on privacy, the extent to which those requirements change current State driver's licensing practices, and how DHS intends to address privacy concerns regarding the Act. This analysis will address the three key privacy issues posed by the Act: (1) The connectivity of the databases; (2) the protection of the personal information stored in the State databases; and (3) the protection of the personal information stored on machine readable technology on the DL/IDs. We invite comments on whether the steps outlined below and otherwise discussed within the NPRM are appropriate and adequate.

1. Connectivity of Databases Mandated by the Act

One voiced privacy concern regarding the Act is that it will create a national identity card and centralized database on all drivers. This concern stems from the provisions in the Act requiring that the individual States electronically verify application information against Federal databases and provide State-to-State access to verify that each applicant only holds a valid license in one jurisdiction. DHS envisions that the operation of both the State data query of Federal reference databases and the State-to-State data exchanges will be left to the States, as is currently the practice in driver's licensing.

As discussed below and in section II.E.6 of the NPRM, the recommended architecture for implementing these data exchanges does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the States. Moreover, no Federal agency will operate the data exchanges affecting non-commercial driver's licensing.[5]

a. *The State Data Query of Federal Reference Databases.* Section 202(c)(3)(A) of the REAL ID Act requires that, before issuing a license or ID, a State verify with the issuing agency, the ''issuance, validity, and completeness of each document required to be presented.'' Given that it is very difficult to validate that the source documents provided by applicants are genuine and have not been altered, certain identifying data contained in the source documents will be checked against authoritative Federal databases as described in more detail in section II.E. of the NPRM.

As described in section II.E., many State DMVs already access one or more of these databases as part of their current licensing processes. The fact, however, that this data verification may now be done by all 56 jurisdictions heightens privacy concerns. The proposed rule seeks to address many of these issues by leaving the operation of this data query, including the development of the business rules, to the States. The rule proposes to require individual States to document their business rules for reconciling data quality and formatting issues and urges States to develop best practices and common business rules by means of a collective governance structure.

A very important example of how administration of this data query will be left to the States is the commitment by DHS to support the development of a ''federated querying service'' to enable the States to access the Federal reference databases in a timely, secure, and cost-effective manner. (See section II.E.6.) Most States already query some of these reference databases either directly or indirectly through a portal provided by AAMVA. DHS is committed to the expedited development and deployment of a common querying service to facilitate the State DMV queries for REAL ID data verification.

To address the privacy concerns posed by such a service, the NPRM makes clear that this service will only enable State DMVs to query Federal systems. The purpose of this federated querying service will be to minimize the impact of data verification on State DMV business processes and reduce the costs of data access. So while DHS will support the development of a querying service, it will not operate this service.

Moreover, use of this federated querying service will be voluntary, and States may choose to maintain or establish direct access to the reference databases; combine direct access with partial use of a common service; or verify applicant data against the reference databases in some other manner. The proposal by DHS to leave the operation of licensing verification with the States should resolve concerns about a centralized database operated by the Federal Government.

In addition, as part of the State certification mandated by section 202(a)(2) of the Act, each State will be required to prepare a comprehensive security plan for its DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses. As part of this requirement, DHS will require that each State include in its annual certification information as to how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents.

b. *The State-to-State Data Exchange.* Section 202(d)(12) of the Act mandates that States provide electronic access to information contained in the motor vehicle database of the State to all other States; and section 202(d)(13) requires that the State motor vehicle database contains, at a minimum, all data fields printed on driver's licenses and identification cards, and motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on licenses.[6] These two provisions mandate the State-to-State data exchange, however, the NPRM contemplates that the States will work out the business process and data access rules necessary to implement these provisions prior to May 11, 2008 by means of a collective governance structure.

[3] The Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act. This is in sharp contrast with the express authorization provided in section 7212 of IRTPA, which was the prior state licensing provision repealed by the Real ID Act. Section 7212(b)(3)(E) of IRTPA stated that the Federal regulations ''shall include procedures and requirements to protect the privacy rights of individuals who apply for and hold driver's licenses and personal identification cards.''

[4] Pub. L. 103–322 as amended by Pub. L. 106–69, 18 U.S.C. 2721 *et seq.*

[5] The database connectivity mandated by the REAL ID Act is in addition to the database connectivity/functionality required to implement the Department of Transportation's existing control over commercial driver's licensing. In addition, law enforcement already have access directly to a State's driver history via the National Law Enforcement Telecommunication System (NLETS), which is the International Justice & Public Safety Information Sharing Network, a message switching system serving the criminal justice community. NLETS is a not-for-profit organization owned and governed by the States.

[6] The information available in each jurisdiction's database varies, but generally they already store what is required by the Act.

As described in section II.E., below, although the REAL ID Act creates a requirement for this State-to-State data exchange, such an exchange already exists under the Department of Transportation's (DOT) rules and regulations governing commercial driver's licenses (CDLs) and State connections to the National Driver Register (NDR)/Problem Driver Pointer System (PDPS) and the Commercial Driver's License Information System (CDLIS).[7] These systems exchange information about commercial motor vehicle drivers, traffic convictions, and disqualifications.

A State uses both the NDR/PDPS and CDLIS to check a driver's record, and CDLIS to make certain that the applicant does not already have a CDL. Under these programs, as well as the REAL ID Act, the primary purpose of the State-to-State data exchange is to determine if the applicant is unqualified and the application fraudulent; the purpose is not specifically to verify the applicant's identity.

The existing State-to-State data exchange among DMVs, while focused on commercial driver's licensing, also impacts non-commercial license applicants, as States are currently required to run all license applicants against the PDPS and CDLIS, which are both pointer systems that collect limited information from each State in order to match against the incoming inquiries. Both systems offer some mandatory privacy protections. The PDPS is subject to Federal regulations 23 CFR 1327.1 *et seq.*, which adopts the Privacy Act of 1974 [8] principles of individual participation and collection, use, and disclosure limitation.

DHS intends to work closely with the DOT, AAMVA, and the States to fulfill the requirements for State-to-State data exchange under the REAL ID Act, while also supporting privacy protections for this exchange. It has not been determined whether CDLIS or some other service will be the platform for the State-to-State exchange, but regardless of the platform, it will be necessary for the States, working with DHS and DOT, to define the privacy protections for any State-to-State data exchange. DHS and DOT will collaborate with states on the privacy protections and access provisions for any State-to-State data exchange.

For example, with support from the DHS Privacy Office, representatives of the DMVs of California, Iowa, Massachusetts, and New York formed a Federation in July 2006 to identify a collective governance structure for the State-to-State data exchange and to begin to develop business rules, including privacy protections. This Federation has recently joined with the AAMVA REAL ID Steering Committee to develop an independent governance structure for the State-to-State data exchange. The development of privacy protective business rules, standards, and governance mechanisms will be central to ensuring that the privacy of license holders is protected.

2. Protection of the Personal Information Stored in State Databases

As discussed at the outset of this section, the DPPA only addresses disclosure of motor vehicle record information but does not address the security of the motor vehicle record information or databases. The REAL ID Act, however, calls for DHS to issue regulations that ''ensure the physical security of locations where licenses and identification cards are produced and the security of document materials and papers from which driver's licenses and identification cards are produced.''

DHS believes that this language provides authority for it to define basic security program requirements to ensure the integrity of the licenses and identification cards. The NPRM, therefore, proposes that each State submit as part of the REAL ID Act certification process a written, comprehensive, security plan. This requirement provides an important safeguard for the personal information collected, maintained, and used by State motor vehicles offices, and it will help assure the public that their information is being handled appropriately. (See NPRM section II.K., below.)

As part of its security plan, each State is also required to outline how the State will protect the privacy of personal information collected, disseminated or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft. Each State must prepare these plans to cover all State DMV offices and driver's license storage and production facilities, databases and systems and submit them as part of its comprehensive security plan.

The State's certification should demonstrate that it has implemented best practices to protect the privacy of the license holder as guided by the fair information principles, which call for openness, individual participation (access, correction, and redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing. These principles are widely recognized and embodied in numerous Federal, State, and international law and codes of practice.

DHS requests comments on recommended best practices for protecting the privacy of the personal information stored in the various State motor vehicle databases pertaining to the requirements under this Act.

3. Protection of the Personal Information Stored in the Machine Readable Technology

The REAL ID Act standardizes the minimum personal information on REAL ID driver's licenses and identification cards, and mandates a machine readable technology. DHS is sensitive to the privacy concerns raised by the potential for non-governmental third parties to collect and use the personal information on REAL ID driver's licenses and identification cards. As discussed in sections II.H.7–9, DHS is recommending that States use the PDF–417 2D bar code and DHS leans toward recommending that States protect the personally identifiable information stored in this 2D bar code by requiring encryption, if the operational complexity of deploying a nationwide encryption infrastructure to process access by law enforcement can be addressed.

4. Conclusion

In summary, DHS has proposed the following privacy protections in its implementing regulations for the REAL ID Act: (1) The State-to-State data exchanges and the State data query of Federal reference databases will be State operated and governed; (2) as part of the State certification process, States will be required to submit a comprehensive security plan, including information as to how the State implements fair information principles; and (3) while acknowledging the benefits of employing encryption of the personal information stored on the identification cards, we invite comment on its feasibility and costs and benefits to ensure that its costs do not outweigh the benefits to privacy.

These protections are intended to serve as a floor and do not prevent the States from using their own statutory or executive authority to provide additional privacy protections, consistent with Federal law, for the personal information stored on the REAL ID licenses and in their databases. DHS intends to work closely with the States as they develop the information

[7] CDLIS was developed to enable record checks of the nation's professional truck and bus drivers. It is an enhanced pointer system that requires States to update records and exchange data.

[8] The Privacy Act of 1974, 5 U.S.C. 552a.

system(s) necessary for querying appropriate Federal and State databases to verify the information contained in the source documents and to determine lawful status of applicants. DHS expects that any system developed for purposes of the REAL ID Act will build in appropriate privacy and security mechanisms to reduce the risk of unauthorized access, misuse, fraud, and identity theft.

DHS believes that protecting the privacy of the personal information associated with implementation of the REAL ID Act is critical to maintaining the public trust that Government can provide basic services to its citizens while preserving their privacy. DHS recognizes the significant privacy issues that are associated with the Act. The public is encouraged to comment on the privacy and security issues associated with implementation of the Act in order to ensure that the final rule implementing this statute reflects sufficient public input on these important issues, which could include the requirements of State comprehensive security plans; access to information collected by States pursuant to the REAL ID Act and the protection of such information stored in State databases; and the operation and governance of electronic verification by States of driver's license application information.

D. Document Standards for Issuing a REAL ID Driver's License or Identification Card

Section 202(c)(1) and (2) of the Act requires that States issuing REAL ID driver's licenses and identification cards obtain and verify from applicants documentation establishing—

(1) The applicant's identity, through a photo identity document, or a non-photo identity document that includes full legal name and date of birth if a photo identity document is not available;

(2) Date of birth;

(3) Proof of SSN or ineligibility for an SSN;

(4) The applicant's address of principal residence; and

(5) Lawful status in the United States.

Currently, every State has a different list of the kind and number of acceptable identification documents. Many are voluminous, encompassing 40 or 50 different types of documents. Many States utilize a ''points'' system where a combination of documents accumulating a sufficient number of ''points'' is deemed sufficient. Others use a tier system of ''primary'' and ''secondary'' documents, where, for example, a primary (such as a passport) and a secondary (such as an electric bill confirming an address) are required.

Driver's licenses are the documents used most frequently to establish identity and often serve as source documents to obtain other forms of identification. If an individual obtains a fraudulent driver's license or identification card, he or she can potentially engage in identity-based fraud, or even obtain access to areas and facilities where he or she might cause harm or otherwise pose a severe risk to security.

Based on these considerations, DHS has determined that many of the documents currently accepted by DMVs and proposed by others are not sufficient to address Congress' direction to enhance national security. Many of the documents on these lists can easily be counterfeited, or their authenticity cannot be easily verified by the States—especially outside of the State of issuance. Therefore, this rule proposes a short list of acceptable documents for REAL ID and temporary REAL ID driver's licenses and identification cards.

This approach offers several advantages from a security perspective. First, restricting the number of documents means that only the documents which DHS has found to be the most secure are chosen to demonstrate identity. Second, limiting the number improves the chances that DMV employees will be able to distinguish valid from fraudulent documents because there will be fewer categories of documents with which they will need to be familiar. Third, a smaller list of documents increases the ease of verifying the documents independently, a related statutory requirement and one that will be very effective in reducing document and identity fraud.

Under the NPRM, DHS proposes that States require that applicants provide at least one of these documents in order to obtain a REAL ID driver's license or identification card. States could add additional documentation requirements to satisfy their own objectives, but at least one of the documents listed below would have to be presented for every application. State agencies would not be required to comply with these requirements when issuing driver's licenses or identification cards in support of the Federal Witness Security Program, codified at 18 U.S.C. 3521 *et seq.*, or operations by other Federal, State, or local criminal justice agencies. In addition, when requested by an authorized representative of the Federal Witness Security Program or the criminal justice agency, States should remove from public records appropriate material relating to the prior or other identities of people involved in the operation and should take sufficient other steps, as directed by appropriate officials, to safeguard the identities of such persons.

1. Documents Required for Proving Identity

The list of acceptable documents that DHS proposes to establish identity for purposes of this regulation is as follows:

- A valid unexpired U.S. passport.[9]
- A certified copy of a birth certificate.
- A consular report of birth abroad.
- An unexpired permanent resident card.
- An unexpired employment authorization document (EAD).
- An unexpired foreign passport with valid U.S. visa affixed.
- A U.S. certificate of citizenship.
- A U.S. certificate of naturalization; or
- A REAL ID driver's license or identification card issued subsequent to the standards established by this regulation.

a. *A Valid Unexpired United States Passport.* A U.S. passport is issued only by the U.S. Department of State (DOS). It may be issued only to United States citizens or nationals. If issued for the full validity period (ten years for adults; five years for minors under 16 and for diplomatic and official bearers) it is statutory proof of U.S. citizenship during its period of validity. Before a U.S. passport is issued, the written application is carefully adjudicated to establish the citizenship and identity of the bearer. First-time applicants must appear in person. A U.S. passport has security features that include special paper, inks and photo printing that make it difficult to counterfeit or alter. Beginning in 2006, U.S. passports also contain the additional security feature of an integrated circuit chip containing the bearer's bio-data, a biometric, and unique chip identification information.

b. *Certified Copy of a Birth Certificate Issued by a U.S. State or Local Office of Public Health, Vital Records, Vital Statistics or Equivalent.* DHS recognizes that a birth certificate is not an identity document in the true sense of the term. Instead, a birth certificate is a record that a birth took place at a particular time and place, and nothing (such as a photograph or other biometric) ties a particular person to a particular birth

[9] A passport also includes the passport card that the Department of State announced in its Notice of Proposed Rulemaking published October 17, 2006 concerning the Western Hemisphere Travel Initiative (WHTI) (71 FR 60928).

certificate. However, section 202(c)(1)(A) of the Act states that a non-photo identity document is acceptable, if it includes the person's full legal name and date of birth. DHS believes that this strongly suggests that Congress intended to maintain the use of the birth certificate for this purpose, recognizing the longstanding practice that birth certificates are used to obtain driver's licenses and identification cards. DHS also understands that the vast majority of driver's license and identification card applicants may only have a birth certificate available for this purpose; while U.S. citizens could use a U.S. passport, passports are currently held only by an estimated 25 percent of Americans.

To achieve security objectives, DHS is proposing that only certified copies of birth certificates that include the individual's full name and can be verified by a State vital statistics, public health, or similar office would be acceptable. Interpreting this more broadly could result in a myriad of non-secure, non-verifiable documentation being used to obtain a driver's license or identification card. Given the fact that Congress specified that the requirements enumerated in section 202(c)(11) were a ''minimum,'' and given also the serious security implications associated with other implementation considerations included in Title II of the Act, DHS believes that it has the necessary authority to interpret this clause narrowly. Accordingly, this regulation interprets section 202(c)(1)(A) to mean only a certified copy of a birth certificate, and only one issued pursuant to the other requirements discussed in this section. These regulations do not preclude a State that accepts a birth certificate as the applicant's identity document from requiring the individual to also present one or more forms of photo identification to substantiate his or her claimed identity.

A corollary issue considered by DHS is whether to recognize delayed birth certificates issued more than one year after the birth itself. While these cases are relatively few, States have established procedures in place for adjudicating these claims and require evidence to prove the actual occurrence of the birth prior to issuing the birth certificate. Therefore, delayed birth certificates lawfully issued by the States will also be acceptable as an identity document.

c. *DOS Consular Report of Birth Abroad of a Citizen of the United States, FS–240; and DS–1350 and FS–545.* The Consular Report of Birth Abroad (CRBA), FS–240, is a document issued by a United States consular officer to a person born abroad who acquired United States citizenship at birth. It is statutory proof of U.S. citizenship. The parent of a child acquiring U.S. citizenship at birth abroad must apply for the CRBA before the child's 18th birthday, and must document the child's acquisition of U.S. citizenship. The CRBA is printed on secure paper in a format that resembles a state birth certificate. There are two other DOS documents issued for U.S. citizens born abroad and acquiring U.S. citizenship at birth. Certifications of Report of Birth Abroad (DS 1350), issued only by Passport Services Vital Records Office, may be accepted as the equivalent of the CRBA. Certifications of Birth (FS–545) issued at U.S. Foreign Service posts prior to November 1990 but no longer issued are still valid and list only the child's name, date of birth, place of birth, and recording date.

d. *Certificate of Naturalization, Form N–550 or N–570, or Certificate of Citizenship, Form N–560 or N–561.* The Certificate of Naturalization is issued by the United States government as proof of a person having obtained U.S. citizenship through naturalization (a legal process of obtaining a new nationality). The Certificate of Citizenship is proof of an individual having obtained U.S. citizenship through derivation or acquisition at birth. These documents are currently issued by DHS, printed on secure paper and have a photograph attached.

e. *Unexpired Permanent Resident Card, Form I–551.* This document, also known as a ''green card,'' is issued by DHS to lawful permanent residents of the United States. The current version contains numerous security features, such as microline printing and a digital photograph. While most of these documents display an expiration date, the status itself does not expire.

f. *Unexpired EAD, Form I–766 or Form I–688B.* This document is issued by DHS to numerous categories of aliens in the United States who are lawfully authorized to work. The Form I–766 document is secure and difficult to counterfeit. The I–688B is expected to be phased out by 2008, but under this proposal would be acceptable until it is phased out.

g. *Unexpired Foreign Passport with valid U.S. visa affixed.* Valid unexpired passports from around the world have traditionally been acceptable documentation to establish identity in most, if not all, States. Most passports meet certain international standards criteria for security as defined by the International Civil Aviation Organization (ICAO). Security features for these documents include digital photographs, information stored on a machine-readable zone, and other forensic features. Some passports issued by foreign countries, however, do not have these features, and can even be hand-written. DHS was concerned about requiring the States to maintain knowledge of passport types from all around the world in order to be able to combat fraud. Further, DHS believes that DMVs, once they verify the visa, should be permitted to rely on the fact that, in issuing the visa and admitting the alien to the United States, the Departments of State and Homeland Security have verified the passport to the extent required by the REAL ID Act (*see* section 202(c)(3)(A) of the Act, and subsection II.E. of this preamble, below).

Accordingly, States may accept a U.S. visa contained in a foreign passport as an acceptable means of authenticating identity. Not only are the U.S. visas secure and contain a photograph, issued U.S. visas can be verified against DOS systems electronically using the same connectivity required to verify U.S. passports.

DHS is aware that inclusion of a visa alone will leave a large group of aliens who have lawful status in the United States unable to obtain a document that is on this list. First, this includes those nonimmigrants admitted under section 217 of the Immigration and Nationality Act (the Visa Waiver Program, or VWP), as well as the Guam visa waiver program. However, these aliens are admitted solely for short periods of time, are prohibited from working in the United States, and are unlikely to qualify for a U.S. driver's license under typical State residency requirements. Further, these aliens can typically use either the driver's license from their home country or an international driver's license to be able to drive a car while lawfully in the United States. Also, they will still be able to obtain a non-REAL ID license (if the State permits it) that could be used for driving purposes, but not for official Federal purposes pursuant to this regulation. Overall, DHS does not believe that this policy would significantly impact VWP aliens.

Another classification of persons that would be unable to present a visa are Canadians who enter the United States without having to obtain a visa and who stay in the United States for extended periods (*i.e.*, more than 90 days) at a time. While the majority of these are short-term visitors who would not need a U.S. driver's license, and indeed are not issued any U.S. documentation or recorded in U.S. nonimmigrant data systems, some are longer-term visitors

who may be students, authorized workers or others who may have reason to need a U.S. license. DHS requests comments specifically on how this group could be affected if they are unable to obtain a U.S. REAL ID driver's license that could be used for Federal purposes.

h. *Driver's License/Identification Card Issued After the Standards Established by the Regulation.* Any REAL ID driver's license or identification card issued after the establishment of these new standards, except non-REAL ID driver's licenses and identification cards issued under section 202(d)(11) of the Act, should be acceptable to establish identity, when an individual moves from State to State or when a driver's license or identification card is being renewed.

2. Additional Documents Considered and Rejected for Proof of Identity

a. *Transportation Worker Identification Credential.* One document considered by DHS as acceptable to demonstrate identity is the Transportation Worker Identification Credential (TWIC). This identification document will be very secure and those who obtain it will be subjected to rigorous background checks. However, DHS believes that any identification document acceptable in this regulation must be capable of being verified electronically by a State in a timely fashion. Including a TWIC on the list of acceptable identity documents, at this time, would require DHS to develop, and the DMVs to access, information electronically using a system that has yet to be created. All TWIC holders would also have one of the other documents prescribed by the regulation. Thus, DHS is not at this time proposing to include the TWIC as an acceptable identity document for REAL ID driver's licenses and identification cards.

b. *Department of Defense's Common Access Card.* DHS also considered the Department of Defense's Common Access Card (CAC). The CAC card may prove convenient for members of the military who move frequently and need to get new driver's licenses and identification cards. For the same reasons as the TWIC, DHS is not proposing to include this document on the list at this time. DHS does not dispute the quality or utility of the CAC; however, DHS believes that any CAC holder would also have one of the other documents on the DHS proposed list, and including the CAC card would require States to connect to additional Federal databases for verification purposes, without sufficient justification.

c. *Native American Tribal Documents.* DHS discussed these documents with the Bureau of Indian Affairs of the Department of the Interior and concluded that since all tribes obtain State-issued documentation to verify birth, all tribal members will have, or can obtain, an eligible identification document, rather than using tribal documents.

DHS solicits comments on whether these or any other documents should be included as acceptable documentation for showing identity. Commenters should address instances in which classifications of individuals could not obtain any of the documents already on the proposed list, issues of reliability of the document proposed, and ability of the States to verify the proposed document. If DHS concludes that other documents, including those listed above and others submitted by commenters, are reliable and can be verified electronically by the States, they may be included as acceptable identity documents in the final REAL ID rule.

3. *Other Documentation Requirements.* In addition to presenting evidence of identity, the Act requires that a driver's license or identification card applicant present the following:

a. *Documentation Showing Date of Birth.* Individuals may use all documents included on the list of identity documents to demonstrate date of birth. Thus, while this is a statutory requirement, it is fulfilled by presenting one of the documents already required under the proposed list of identity documents.

b. *Evidence of a SSN or Proof of Ineligibility.* The United States, on both Federal and State levels, has experienced significant amounts of fraud due to the misuse of SSNs. Much of this has been in the context of ''identity theft'' or other financial crimes. However, the misuse of SSNs can have a national security impact as well. For example, many of the September 11, 2001 (9/11) hijackers used numbers that were either never issued by the Social Security Administration (SSA), were issued in the name of a child, or had been associated with multiple names. The hijackers used this information to obtain driver's licenses, and some held multiple driver's licenses from States including Virginia, Florida, California, Arizona, and Maryland.[10] Accordingly, DHS believes that the congressional mandate to check all SSNs against SSA databases prior to the issuance of a REAL ID driver's license or identification card will increase security and decrease the ability to obtain driver's licenses fraudulently. This will not be a significant burden to the States as almost all jurisdictions currently verify SSNs against SSA databases, 46 States using Social Security On-Line Verification (SSOLV).

SSA has taken significant steps since 2001 to strengthen the SSN issuance process. SSA has a plan for improving the security of the SSN card itself, in compliance with section 7213 of the Intelligence Reform and Terrorism Prevention Act of 2004. In recognition of improvements in the SSN issuance process and plans for improving the security of the SSN card, DHS considered requiring DMVs to require individuals to present a social security card with their full name and SSN as the only mechanism to demonstrate evidence of their SSN.

DHS recognizes, however, that this approach would be costly and would create an undue hardship on SSA and the public, particularly on members of the public who had lost or misplaced their social security cards. Accordingly, DHS proposes to allow an applicant to establish his or her SSN by presenting his or her social security card, a W–2 form, a SSA–1099 form, a non-SSA 1099, or a pay stub with the applicant's name and SSN on it.

An alien in the United States without authorization to work is generally not eligible for an SSN. Thus, to prove ineligibility for an SSN, an alien must present evidence that he or she is currently in a non-work authorized non-immigrant status.

c. *Documentation of Address of Principal Residence.* There are a number of potential ways to define the term ''principal residence.'' DHS reviewed State definitions of this term and did not find a consistent definition. The NGA observed that State laws vary widely on how to define residency/domicile because a mobile society leads to frequent relocations, ownership of multiple properties, as well as lifestyles that include no fixed address. Accordingly, DHS proposes to use the *Black's Law Dictionary* definition of ''domicile'' which DHS believes captures the intent of the principal residence requirement of the Act:

The place at which a person has been physically present and that the person regards as home; a person's true, fixed, principal and permanent home, to which that

[10] Testimony of James Huse, Jr. Inspector General, Social Security Administration, House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security; and Subcommittee on Immigration, Border Security, and Claims, 107th Cong., 2nd Sess., June 25, 2002.

person intends to return and remain even though currently residing elsewhere.[11]

The need to determine an individual's principal residence prior to issuance of a REAL ID driver's license also has its origins in the 9/11 terrorist activity. Seven of the 9/11 hijackers fraudulently obtained driver's licenses in the Commonwealth of Virginia, although none of them actually lived there, by providing false information as to their true place of residence. At the time Virginia allowed only a ''signed affidavit'' of a Virginia resident to suffice as proof of residency in the State, and two of the hijackers paid an illegal immigrant (who had himself obtained a driver's license fraudulently) $100 to vouch for them.[12] By September 21, 2001, Virginia had eliminated this loophole.

DHS recognizes that some individuals do not have a fixed address, as that term is commonly used. Individuals who do not have a fixed address, such as the homeless, may still obtain a REAL ID driver's license or identification card if they otherwise can produce the documents a State must possess and verify prior to issuing a REAL ID driver's license or identification card. For such individuals, a State may issue REAL ID driver's licenses and identification cards by adhering to a written exceptions policy as described in section II.F. below.

d. *Evidence of Lawful Status in the United States.* The REAL ID Act specifies the scope of lawful status in the United States for purposes of eligibility for a REAL ID driver's license or identification card acceptable for official purposes. The applicant must be a person who: Is a citizen or national of the United States; is an alien lawfully admitted for permanent or temporary residence in the United States; has conditional permanent resident status in the United States; has an approved application for asylum in the United States or has entered into the United States in refugee status; has a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States; or has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for LPR or conditional permanent resident status.

A U.S. passport, certified copy of a birth certificate, DOS consular report of birth abroad, certificate of citizenship, certificate of naturalization or a permanent resident card can be used to establish lawful status in the United States for purposes of this proposed regulation. If an applicant presents an employment authorization document (Form I–766) or a foreign passport with a valid U.S. visa and/or DHS nonimmigrant Form I–94 affixed for identification, these documents may be accepted as provisional evidence of lawful status, pending verification of status through the Systematic Alien Verification for Entitlements (SAVE) system (*see* section II.E.3 below). Note that while all documents presented must be verified through SAVE or otherwise, the difference is that since a visa or EAD are not necessarily linked to an authorized status, their acceptance is deemed provisional pending confirmation of exact status through further verification. DHS considered, but rejected, requiring additional documentary evidence of status that may be issued by DHS, but considered this requirement unworkable, particularly since many holders of EADs simply do not have any other consistent, reliable identification.

The EAD is envisioned as the document to be presented by the following classes of REAL ID-authorized aliens: Temporary Protected Status (TPS) aliens; asylees and asylum applicants; refugees; adjustment applicants; and aliens granted deferred action. DHS understands that regulatory limitations on issuance of EADs to asylum and TPS applicants will result in a wait period before these aliens will have acceptable documentation, and invites comment on what alternative documentation regimen may serve for these groups, and whether those groups need a REAL ID driver's license or identification card before their applicable wait period expires.

The proposed rule also does not include immigration documentation showing any status under the immigration laws of American Samoa or the Commonwealth of the Northern Marianas for aliens within those jurisdictions. REAL ID specifies U.S. immigration statuses. DHS invites further comment about how these jurisdictions may better be integrated into the REAL ID framework.

E. Verification of Information Presented

Section 202(c)(3)(A) of the Act requires verification from the issuing agency for issuance, validity, and completeness of documentation to establish the following:

- Identity.
- Date of birth.
- Proof of SSN, or that the person is not eligible for an SSN.
- The person's name and address of principal residence.
- The person's lawful status in the United States.

The documents that individuals are required to present are described in section II.D.1 and are listed in § 37.11 of the proposed regulation.

To verify with the issuing agency, the issuance, validity, and completeness of documentation means that the State must determine independently that the document itself has been legitimately issued by the issuing agency to the individual presenting the document, prior to issuing the driver's license or identification card to the individual.[13] This means that DMVs are required to perform a physical inspection of the source document to ensure that it appears authentic and has not been tampered with. However, document verification is not sufficient. DMVs must also verify the information contained in the document with an authoritative or reference database. Thus, States must verify both document and data under the Act, although this verification may be phased in over time.

The use of the phrase ''required to be presented by the person under paragraph (1) and (2)'' in section 202(c)(3)(A) of the Act means that only the specific documents required by this proposed regulation need to be verified. Thus, in the case of identity, only the documents listed in these regulations as required to be presented must be verified. If States wish to require additional documentation to prove identity—for example, if they wish to require photo identification in addition to a certified copy of a birth certificate—then the State does not need to independently verify these additional items, only the birth certificate, as it is included on the Federal list. Ensuring that at least one document presented is independently verified will increase security by reducing the ability to fraudulently manufacture documentation typically used to obtain driver's licenses and identification cards.

Requiring additional documentation can help a State to confirm the identity (or address, or whatever fact is at issue)

[11] Bryan A. Garner, editor, *Black's Law Dictionary,* 8th ed., p. 523 (Thomson-West, 2004).

[12] Testimony of Paul McNulty, United States Attorney, Eastern District of Virginia, House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security; and Subcommittee on Immigration, Border Security, and Claims, 107th Cong., 2nd Sess., June 25, 2002.

[13] See discussion infra at II.J.2 on verification of birth certificates through the Electronic Verification of Vital Events system (EVVE). If this system is not operational by May 11, 2008, a State must verify the validity of the birth certificate at the first license renewal or re-issuance once EVVER is available.

of a person. This is a common method used now by many States—the idea of ''cross-verifying'' data elements included on different documents. However, each independent verification of a document can cost time and money for the DMVs—which can create a disincentive to require many documents to prove identity and thus eliminate the benefits of this cross-verification. If this regulation proposed to require that all documents presented for any purpose be verified, this would be an incentive for States to require only the one document that the REAL ID regulation requires. In that circumstance, the verification requirement could result in a less secure process. DHS believes that the better and more secure solution is to require that a State verify the identity document an applicant presents, pursuant to REAL ID requirements. States retain the flexibility to require documents in addition to the Federal document requirements, and to verify them pursuant to their own regulations and practices. Any additional documents beyond those listed in § 37.11 need not be verified independently, but can be ''cross-verified'' against the one document that must be verified according to these regulations. DHS proposes that it be up to the States whether to keep digital or paper copies of supplemental documentation beyond the Federal document requirements, pursuant to the retention requirements discussed in this regulation.

1. Verification of ''Address of Principal Residence''

Although the Act requires States to verify an applicant's ''address of principal residence,'' DHS believes that there is no nationally available, reliable, up-to-date, and cost-effective method for States to verify this information with the issuing source of the document, as the plain language of the Act would seem to require. DHS examined existing governmental and non-governmental databases that alone, or in combination, could be used by States to fulfill this requirement, and determined that there is no single way for States to comply with this requirement by May 11, 2008, or in the reasonably foreseeable future.

States currently have widely varying ways of determining a person's residence, although all States require an applicant to demonstrate that they live in the State in which they are applying for a driver's license or identification card. While the U.S. Postal Service can do a basic electronic check for a fee, this system is based on nothing more than the applicant or some unrelated individual sending to the post office a change of address card. Thus, although an electronic verification, it is not based on reliable information.

Further, in almost all cases there is no way to verify independently from documents presented that an address is a person's principal address. A mortgage statement or lease may indicate that a person owns or rents property in a particular place, and while the landlord or bank holding the mortgage could verify this, it does not establish that this is the person's principal residence, just that the ownership or rental is legitimate. In addition, the cost to States of verifying a multitude of documents presented to establish address, such as utility bills, leases, mortgages, or other documents, is potentially significant.

In spite of these limitations, there is a need for some reliability in the information presented for principal residence, as evidenced by the experience of the 9/11 hijackers and how they obtained Virginia driver's licenses (*see* section II.D.3). Therefore, DHS is proposing that the States require each applicant to present at least two documents that include his or her name and current principal residence. However, the States will retain the flexibility to determine for themselves precisely which documents, or combination of documents, an applicant must present to satisfy this requirement and how a State will validate or verify this information. The proposed regulation would require States to establish a written policy identifying acceptable documents and how, or if, they will be independently validated or verified. The proposal would also require that States provide this information to DHS as part of their initial certification package and whenever this policy is modified or superseded.

While States are free to determine the list of acceptable documents for themselves, whatever documents individuals submit must contain a street address for individuals where available. Post office boxes or rural route numbers are not acceptable addresses, since the statute requires a residence, not simply an address.[14] Documents issued monthly (*e.g.*, bank statements, utility bills) could not be more than three months old at the time of application. Documents issued annually (*e.g.*, property tax records) would need to be for the most current year at the time of application.

Applicants would also be required to sign a declaration (that could be included as part of the driver's license or identification card application form) affirming that the information presented is true and correct, including information presented to establish address of principal residence. For minors and other dependents, parents or legal guardians would submit the documentation establishing a principal residence on behalf of the driver's license or identification card applicant. The parent or legal guardian would need to present photo identification (that the DMV would need to verify) and would be required to submit two or more address documents, as if he or she were the primary applicant, and sign the affirmation.

2. Verification of Identity Information

a. *Certified copy of a Birth Certificate Issued by a U.S. State or local office of Public Health, Vital Records, Vital Statistics or equivalent.* DHS anticipates that the States will be able to verify electronically the issuance of a birth certificate through the Electronic Verification of Vital Events (EVVE) system. Once functional, this system will be able to verify that the information presented on a certified copy of a birth certificate is a match to a vital statistics birth record, in response to an electronic query from a State DMV. While the EVVE system has not been tested nationwide, the National Association of Public Health Statistics and Information Systems (NAPHSIS) has informed DHS that such a system could be in place and fully operational by May 2008. If such a system is either not available nationally by the effective date of the regulations, or a State is seeking to verify the validity of a birth certificate from a State that is not participating in the EVVE system, a State may establish written procedures for how it will attempt to verify such records, and document its use of those procedures. At a minimum, the applicant's file and/or records should contain a notation that the birth certificate information was not verified electronically with the issuing agency, and such electronic verification will be necessary at the first driver's license or identification card renewal or re-issuance once the information is available for electronic verification. Confirmation of the birth certificate through EVVE will verify not only the person's identity but also provide evidence that they are very likely to be a U.S. citizen and therefore have lawful status in the United States.

As discussed above, individuals born before January 1, 1935, may be unable to produce birth certificates, or States may be unable to verify any birth certificates produced by such

[14] One exception might be American Samoa as this territory does not possess the same type of addresses commonly used in the 50 States.

individuals. Individuals born before 1935 may never have received a birth certificate, and it may not be possible for their birth States to reproduce the document for them. In addition, States may not have birth information available electronically for all births prior to 1935, and DHS believes that it would be too burdensome on States to verify this information in a non-electronic method. Such cases should not preclude persons from obtaining a REAL ID driver's license or identification card, but should be handled according to the State's exceptions process. DHS intends to align this provision with the final rule on minimum standards for birth certificates promulgated by HHS, in accordance with its statutory obligation under section 7211 of the Intelligence Reform and Terrorism Prevention Act (Pub. L. 108–58).

b. *U.S. passports or Consular Report of Birth Abroad issued to U.S. citizens abroad by the Department of State.* It is anticipated that a State will be able to electronically verify a U.S. passport, or a birth certificate issued to a U.S. citizen abroad. The automated system that is eventually developed will confirm that the passport was issued by DOS. In the case of a U.S. passport or a consular report of birth abroad issued by DOS, electronic verification will also confirm that the applicant has lawful status in the United States.

c. *Valid U.S. visas affixed in an unexpired foreign passport.* DHS examined several options in determining how to independently verify a U.S. visa affixed to a foreign passport as required by the REAL ID statute. First, verifying the foreign passport itself with the Government that issued it is simply not feasible. There is no guarantee that a foreign Government would answer a State DMV's request to authenticate a specific document, or any requirement in international law that they do so in a timely manner. Requiring this foreign independent verification would be an unfair burden to both the driver's license or identification card applicant and the State DMV attempting to adjudicate the application.

Recognizing that the U.S. visa affixed in the passport, and not the passport itself, would be the acceptable documentation to demonstrate identity, DHS turned to how that verification would occur. First, DHS examined whether the DMVs could use the State Department systems to verify the visa. While this was a feasible solution since access to DOS databases will ultimately be necessary for all DMVs anyway (to verify U.S. passports and certain birth certificates), authentication of a U.S. visa does not, by itself, establish lawful status in the United States.

While a U.S. visa can be issued for as long as ten years (and often is), it is the Customs and Border Protection (CBP) Officer at U.S. ports of entry who determines the actual admission period for the person seeking to enter the United States. In most cases, this admission period is less than the validity period of the U.S. visa. Accordingly, foreign travelers often use the same visa for multiple trips to the United States—and the length of validity period for the visa is not dispositive as to whether someone has lawful status in the United States. Therefore, to adopt a policy in which a U.S. visa holder must use that visa to establish identity would require that aliens using a U.S. visa as evidence of identity have to undergo three separate checks—the DOS database (to confirm identity), SAVE (to confirm lawful status), and SSOLV (to confirm the Social Security Number). All other categories of driver's license or identification card applicants, including U.S. citizens (whether born in the U.S. or abroad), LPRs, and others would require only two database checks. This approach was deemed to be unduly burdensome on both the applicant and the DMV.

DHS then considered another solution—validating the U.S. visa through existing U.S. immigration and border processing procedures, including DHS's U.S.VISIT and the Department of State's BioVisa Program. Currently, when a person applies for a U.S. visa abroad, he or she is required to submit finger scans, which are biometrically verified when the person arrives in the United States—so that the United States can be sure that the person who received the visa is the same person seeking admission.

DHS believes that, for purposes of obtaining a REAL ID driver's license or identification card, the fact that the U.S. visa was used to enter the United States, and that person was checked against US-VISIT, is an acceptable verification that the document (the U.S. visa) is legitimate. The U.S. visa has been checked against a Government-held database via the biometric check upon arrival. State DMVs will not be required to check the US-VISIT system to confirm that the visa was used for admission. Thus, if the person holding a U.S. visa has lawful status in the United States, which can be verified through SAVE, then the person will have established both identity and lawful status. Under this proposal, aliens presenting a foreign passport with a valid U.S. visa would require only a SAVE and SSOLV check, placing them on par with other driver's license or identification card applicants.

3. Verification of Lawful Status

If an applicant presents a permanent resident card (Form I–551), an EAD (Form I–766), or a foreign passport with a U.S. visa affixed, the applicant is not a U.S. citizen. In accordance with the Act, this proposal would require the States to verify the authenticity of the identity documentation and lawful status in the United States at the same time, using the SAVE system maintained by U.S. Citizenship and Immigration Services (USCIS). Under section 202(c)(3)(C) of the Act, States have already been required to enter into memoranda of understanding with DHS by September 11, 2005, to use the electronic and automated system to verify the legal status of a non-U.S. citizen applying for a REAL ID driver's license or identification card.

SAVE is an existing program within DHS that allows State DMVs (as well as many other Federal, State, and local benefit and license granting agencies) to verify electronically the immigration status of the person applying for a driver's license or identification card. This system can verify that a person presenting a Permanent Resident Card (Form I–551) was issued lawful permanent resident status in the United States and, thus, is lawfully in the country. SAVE can also confirm that a person presenting an EAD (Form I–766 or Form I–688B) is in a lawful nonimmigrant status and present in the United States for a fixed period of time. Moreover, SAVE can confirm that an applicant presenting a U.S.-issued visa affixed to a foreign-issued passport is lawfully in the country for a temporary period of time. If a person presents a U.S.-issued visa affixed to a foreign-issued passport, then the applicant will also need to present additional documentation to allow for a SAVE search. This could be a passport stamp, an I–797 Notice of Action, or some other documentation issued by USCIS. The terms and conditions of access to SAVE by a State, including any costs to be borne by the State, shall be established by memorandum of agreement between DHS and the State pursuant to section 202(c)(3)(C) of the Act.

For student aliens admitted for duration of status (D/S), DMVs should use the Student and Exchange Visitor Information System (SEVIS) for verification. SEVIS is a system in which DHS and schools who enroll foreign students communicate to ensure that the aliens claiming student status (as well

as exchange visitors such as au pairs) are in fact currently enrolled. There will ultimately be a connection between SEVIS and SAVE, but until such time, DHS has decided on the following:

- DHS will use the SAVE/SEVIS connection, if the systems are connected prior to May 2008.
- If the SAVE/SEVIS connection is not available, DHS may require foreign students to present a certified statement from the registrar of the school in a sealed envelope demonstrating that he or she is still in school at the time of the alien's application for a driver's license or identification card (and thus still in lawful status).

Individuals who are denied a temporary REAL ID driver's license or identification card due to a SAVE check that they believe is in error should contact the local USCIS branch, or as USCIS may otherwise direct, to resolve concerns over verification of their lawful status.

4. Verification of Date of Birth

As stated earlier, all of the documents listed on the proposed list of acceptable identity documents display the date of birth on the face of the document. Thus, once the information on the document is verified, as it must be for identity purposes, there is no further need for the States to verify date of birth independently.

5. Verification of Social Security Account Number or Ineligibility

Because of the requirements for the issuance of commercial driver's licenses, the majority of State DMVs already have access to the SSA database for verification of SSNs. Thus, when the DMV applicant presents evidence of an SSN, the DMV will be able to verify that number through existing systems. Verification that a person is not eligible for an SSN must also be provided. To satisfy this requirement, an alien must present evidence, verifiable through SAVE, that he or she is currently in a nonimmigrant status establishing that he or she does not have the right to work in the United States. A person is never permanently ineligible for an SSN, as he or she could obtain some type of immigration status that would entitle him or her to one.

6. Connectivity to Systems and Databases Required for Verification

For individual States to verify information and documentation provided by applicants, each State must have electronic access to multiple databases and systems as described above. DHS considers the deployment of the information systems needed to support the electronic verification of applicant data to be its highest priority. Secure and timely access to trusted data sources is a prerequisite for effective verification of applicant data. Electronic access to the Federally-sponsored databases described above will also significantly reduce the costs of REAL ID driver's license and identification card issuance to States. Finally, DHS will work closely with the States to improve their capabilities for verifying the authenticity of source documents. Both data verification and document authentication are necessary to ensure the validity of REAL ID driver's licenses and identification cards.

a. Applicant Data Verification. Electronic data verification requires secure and timely communications among a number of both Federal and State-sponsored information systems. DHS can provide assistance to states in three key areas: Enhancement of Federally-sponsored reference databases; development of a cost effective service for querying these reference databases; and the exchange of data among states to reduce fraud. While DHS will provide assistance to states in all three areas, its role and responsibilities will differ in each.

i. Reference databases. Confidence in the accuracy and reliability of the data provided by applicants and included on their driver's licenses and identification cards depends in large part on the quality and completeness of data in the reference databases used for verification. These databases, however, are Federally-sponsored and Federally-funded initiatives. Therefore, DHS recognizes that one of its primary responsibilities under the REAL ID Act is to expedite the improvement of the databases required for electronic verification of applicant data. DHS is working with the sponsoring agencies to ensure that the reference databases meet the standards for data quality, reliability, integrity, and completeness required to support REAL ID data verification by the states and other jurisdictions. While some of these reference databases are mature and fully operational, others are still under development and need investments of resources.

First, almost all State DMVs currently access the SSOLV database to verify social security numbers through a portal provided by the American Association of Motor Vehicle Administrators (AAMVA). The quality and reliability of this reference data is good and improving. Second, all fifty states have signed MOUs for access to SAVE and twenty State DMVs are currently querying SAVE to verify lawful status. While secondary queries may be required in some instances to update applicant records in SAVE, more than a million initial queries from State DMV are already being processed each year. Moreover, DHS anticipates that the SEVIS–SAVE connection will be completed before May 2008. Third, DHS is working with NAPHSIS to enhance EVVE functionality and expedite implementation of EVVE in all vital records jurisdictions. Since EVVE is currently in pilot phase and will require states to bring their vital records online, assistance to both NAPHSIS and individual states will be needed. Finally, DHS is working with the Department of State to develop an automated system for verifying data from U.S. Passports, Consular Reports of Birth, and Certifications of Report of Birth. For all of these systems, DHS is committed to improving data quality and data consistency to support timely, cost-effective, and reliable data verification.

ii. *Federated querying service.* States must be able to access the reference databases in a timely, secure and cost-effective manner. As noted above, most states already query some of these reference databases either directly or indirectly through a portal provided by AAMVA. This access, however, needs to be enhanced as the Federally-sponsored systems are upgraded or deployed and all 56 jurisdictions seek access for purposes of applicant data verification. DHS is committed to expediting the development and deployment of a common querying service that will automatically distribute State DMV queries for REAL ID data verification to the appropriate reference databases and combine the multiple responses into a single reply. The purpose of this federated querying service will be to minimize the impact of data verification on State DMV business processes and reduce the costs of data access. DHS will support the development of querying service but will not operate or control this service. DHS is currently exploring alternative solutions. However, use of this federated querying service will be voluntary and States may choose to: Maintain or establish direct access to the reference databases; combine direct access with partial use of the common service; or verify applicant data against the reference databases in some other manner. Finally, DHS and DOT will assist the States in their efforts to develop improved business rules and data formats for data communications with reference databases. These business

rules will, in turn, become part of the security plans submitted to DHS.

iii. *Data exchange among states.* The third area of applicant data verification involves access to other state databases to verify that the applicant is not disqualified from obtaining a REAL ID driver's license or identification card due to possession of a REAL ID driver's license or identification card in another state. Data exchange among states is mandated by section 202(d)(12) of the Act, wherein each State must provide to each other State(s) electronic access to the DMV database of that State. In particular, this rule requires the exchange of data among all jurisdictions to verify that the applicant does not hold a valid driver's license or identification card in another jurisdiction and that other jurisdictions have terminated the applicant's driver's licenses and identification cards before a REAL ID can be issued. However, data exchange among State DMVs is also governed by the National Driver Register Act of 1982, as amended, and the Federal Commercial Motor Vehicle Safety Act of 1986. The Act and this rule pose an additional requirement for State-to-State data exchange, but it does not alter existing rules and regulations. Under all three statutes, the primary purpose of State-to-State data exchange is driver safety—to ensure that drivers are not holding multiple licenses in multiple jurisdictions to avoid points from dangerous driving and to determine if the applicant is unqualified or the application fraudulent—not specifically to verify the applicant's identity. Thus, data exchange among states is substantially different from verification of applicant identity data with the Federally-sponsored databases discussed above. State-to-State data exchange among DMVs is governed by multiple statutes and multiple agency regulations and has been effectuated through multiple database systems. DHS will build upon the existing infrastructure of Federal statutes, regulations, and data systems in implementing REAL ID.

Therefore, DHS will work closely with the Department of Transportation, AAMVA and the States to fulfill the requirements for State-to-State data exchange under the REAL ID Act. DHS will actively support the enhancement and expansion of existing DOT-sponsored systems to meet the requirements of the REAL ID Act. For example, verification that the applicant does not hold a valid driver's license or identification card in another jurisdiction can be accomplished by a variety of methods, including the exchange and comparison of digital image information based on applicant photos. DHS will support such State-to-State exchange initiatives and will partner with DOT, the States and territories, and AAMVA to leverage the value of existing information systems, business rules, standards, and governance mechanisms to facilitate implementation of the Act.

b. *Source document authentication.* In addition to verification of applicant identity data, the Act requires that the jurisdictions authenticate the source documents provided by the applicant. According to section 202(3)(A), ''the State shall verify, with the issuing agency, the issuance, validity, and completeness of each document required to be presented.'' This requires that jurisdictions inspect applicant source documents to ensure that they are genuine and have not been tampered with. DHS recognizes that source document authentication is the responsibility of State DMVs who employ a variety of procedures, both manual and automated, to verify both the overt and covert security features of identity documents. In addition, jurisdictions may institute the exchange of data on identity document security features in order to facilitate the manual or automated inspection and authentication of source documents. DHS will support these State initiatives and require that jurisdictions document their procedures and standards for document authentication as part of their security plans. However, DHS will not support the development of a federally-controlled or operated repository for source documents or a national facility for document authentication under the Act.

F. Exceptions Processing for Extraordinary Circumstances

DHS recognizes that there may be extraordinary circumstances where the required documents verifying an applicant's identity, date of birth, SSN, principal address or lawful status may be unavailable. This would include applicants such as a homeless person with no fixed address, as well as an individual who has lost all documentation to a natural disaster such as Hurricanes Katrina and Rita. In such circumstances, DHS believes that the States should have the flexibility to accept alternative documents to establish a particular data element, provided that the State follows defined, written, procedures that are approved by DHS as part of the State certification process for REAL ID. Therefore, DHS proposes that, where a State chooses to establish an exceptions process, that process must include, at a minimum, the following requirements:

- The driver record maintained by the DMV must indicate when an alternate document is accepted.
- Any driver's license or identification card issued using exceptions processing requires a complete record of the transaction, including a full explanation of the reason for the exception, alternative documents accepted and how applicable information from the document was verified.
- The jurisdiction retains the alternate documents accepted or copies thereof in the same manner as for other source documents as described in section II.J. and provides these upon request to DHS for audit review.

G. Temporary Driver's Licenses and Identification Cards

Aliens who are in the following lawful statuses may receive REAL ID driver's licenses and identification cards: Has a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States; has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for LPR or conditional permanent resident status. However, driver's licenses and identification cards issued to these classes of aliens are only valid for the duration of the person's lawful period of admission, but no more than eight years, or, if there is no fixed date, a period of one year. Further, these ''temporary'' driver's licenses and identification cards must clearly identify on the face of the document that they are temporary.

Renewal of these temporary driver's licenses and identification cards must be in person. The renewal applicant must present valid documentary evidence that the status by which the applicant qualified for the temporary driver's license or temporary identification card has been extended by the Secretary of DHS, or that the individual has qualified for another lawful status category listed in the Act.

The following statuses are indeterminate and will always require issuance of a driver's license or identification card limited to one year: Asylum applicant, TPS applicant, and adjustment applicant. Other temporary categories will vary, and the end of the period of authorized stay, if any, must be verified through the SAVE or other designated verification system. Expiration dates on an EAD are not

necessarily the same as the end date of the status. Visa expiration dates have no relevance to the period of authorized stay. Aliens with immigration statuses other than those designated by REAL ID for temporary driver's licenses and identification cards are not subject to this limitation on the length of their driver's licenses and identification cards, regardless of any expiration date that may appear on their documentation.

H. Minimum Driver's License or Identification Card Data Element Requirements

To meet the requirements of section 202(b) of the Act, a State is required to include, at a minimum, the following information and features on each driver's license and identification card:

(1) Full legal name;
(2) Date of birth;
(3) Gender;
(4) Driver's license or identification card number;
(5) A digital color photograph;
(6) Address of principal residence;
(7) Signature;
(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose;
(9) A common MRT, with defined minimum data elements.

In addition, DHS has determined that States must also include issue date and expiration date on each driver's license or identification card.

Some of these elements are discussed below.

1. Full Legal Name

The intent of this requirement is to improve the ability of law enforcement officers, at all levels of Government, to confirm the identity of individuals presenting State-issued driver's licenses or identification cards. Many States do not have a ''full'' legal name requirement, and using a name other than a full legal name results in ''no matches'' when checked against other public records that use the full legal name. This occurred with some of the driver's licenses and identification cards obtained by the 9/11 terrorists, where the driver's licenses ''names'' were variants on the actual name carried in some of the terrorists' validly issued passports.[15]

This requirement raises several issues. First, the name on the REAL ID driver's license or identification card should be identical to the name shown on the identity document used to obtain the driver's license or identification card. However, formats for recording names on identity documents differ and a driver's license or identification card holder's name may change through marriage, divorce, adoption, or court order. State DMVs currently require appropriate proof in the form of documents indicating an official name change: A U.S. court-or Government-issued marriage certificate, a U.S. court-issued divorce decree, or a U.S. court-issued name change decree. States must require an original or certified copy of one of these documents as proof of change of name, and the document must include either the date of birth or the age of the individual. States must also add the changed name in the motor vehicles record database and not delete any previously captured names so that a complete record of the individual's full name history is present in the motor vehicles database.

With regard to the name placed by the DMV on the face of the driver's license or identification card, DHS is proposing to adopt the ICAO 9303 Standard. The ICAO 9303 standard requires Roman alphabet characters, allows a total of 39 characters on the face of the driver's license or identification card, and provides standards for truncation of longer names.

For the machine readable portion of the card, the machine readable technology standard proposed is the PDF–417 2D bar code (*see* section II.H.8 below). For the machine readable portion of the card, DHS would require States to capture and record up to 125 characters in the bar code and State database to permit capture of the full name history. Allowing at least 125 characters accommodates certain cultures in which multiple, lengthy names, are common and permits greater accuracy in identifying particular individuals.

2. Driver's License or Identification Card Number

Section 202(b)(4) of the Act requires that each REAL ID license or identification card include the person's unique ''driver's license or identification card number.'' Federal law prohibits the display of an individual's SSN on a driver's license.[16]

3. Digital Photograph

Section 202(b)(5) of the Act requires that the State-issued REAL ID license or identification card include a digital photograph of the person. In addition, section 202(d)(3) provides that the State shall require that each person applying for a driver's license or identification card be subject to mandatory facial image capture. This requirement applies whether or not the person is granted a driver's license or identification card. DHS believes that these provisions require each applicant to allow a DMV to take a photograph for the motor vehicle record, and to place the digital image on the face of the driver's license or identification card, if one is issued. If a driver's license or identification card is not issued, DHS is proposing that States dispose of the photograph after one year. The DMV's photo of the individual should be updated with the most recent photograph in the event the applicant reapplies, and any photos taken of the individual prior to successful issuance of the document should be discarded in favor of the photo associated with the successful application. If the DMV does not issue the driver's license or identification card because of suspected fraud, the record should be maintained for ten years and reflect that a driver's license or identification card was not issued for that purpose.

DHS recognizes that some individuals that may apply for a REAL ID driver's license or identification card are opposed to having their photograph taken based on their religious beliefs. However, the Act requires a facial photograph, which serves important security purposes. Given these concerns and the clear statutory mandate, DHS believes that a driver's license or identification card issued without a photograph could not be issued as a REAL ID driver's license or identification card. Many States now issue non-photo driver's licenses or identification cards based on the applicant's religious beliefs. States may continue to issue these driver's licenses or identification cards to such individuals and DHS recommends that these driver's licenses and identification cards be issued in accordance with the rules for non-compliant driver's licenses and identification cards.

DHS is proposing that digital photographs comply with current ICAO standards.[17] Such standards include diffused lighting over the full face to eliminate shadows and ''hotspots,'' a full face image from the crown to the base of the chin and from ear-to-ear (unless the State chooses to use profiles for licensees under 21), and images with

[15] H.R. Rep. No. 109–72 (2005) (Conf. Rep.).

[16] Section 7214 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458, 118 Stat. 3638, Dec. 17, 2004) amended section 205(c)(2)(c)(vi) of the Social Security Act (42 U.S.C. 405(c)(2)(C)(VI)).

[17] The relevant ICAO standard is ICAO 9303 part 1 vol 2, specifically ISO/IEC 19794–5—Information technology—Biometric data interchange formats—Part 5: Face image data, which is incorporated into ICAO 9303.

no veils, scarves or headdresses to obscure facial features, or eyewear that obscures the iris or pupil of the eyes. Photos should also be in color.

4. Address of Principal Residence

This regulation proposes that, in most cases, the individual's principal address be included on the face of the REAL ID driver's license or identification card. DHS proposes exceptions to this requirement, as described below.

a. *Confidential Address.* Section 202(b)(6) of the Act requires that the driver's license or identification card include the person's address of principal residence. Many States have laws that allow addresses to be kept confidential in certain circumstances; for example, where the disclosure of an address may jeopardize the personal safety of such an individual, such as victims of domestic violence, judges, protected witnesses, and law enforcement personnel. Some States provide the standards for address confidentiality through legislation or in their exceptions processing. Most States retain the ''real'' address in their database, but often protect it so that only authorized personnel have access to the ''real'' address. In addition, most States do not have the ''real'' address in the machine readable technology barcode. Rather, the machine readable zone contains only what is on the face of the driver's license or identification card.

Section 827 (Protection of domestic violence and crime victims from certain disclosures of information) of the Violence Against Women and Department of Justice Reauthorization Act of 2005,[18] amended the REAL ID Act 2005 (49 U.S.C. 30301 note), to protect against disclosure addresses of individuals who have been subjected to battery, extreme cruelty, domestic violence, dating violence, sexual assault, stalking or trafficking. Consequently, DHS is proposing to exempt individuals who are entitled to enroll in State address confidentiality programs, whose addresses are entitled to be suppressed under State or Federal law or by a court order, or who are protected from disclosure of information pursuant to section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 from the requirement to have their address displayed on REAL ID driver's licenses and identification cards. DHS understands that other categories of individuals, such as federal judges, may also require that their addresses remain confidential to protect their safety. DHS seeks comment on how these categories of individuals can be protected, while remaining consistent with requirements of the Act.

b. *No Fixed Address.* DHS recognizes that some people do not have a fixed address and that States have exceptions processes in place to address this situation. DHS believes that each State should continue to address these situations through a written and documented exceptions process. For example, in some States homeless people may use addresses of accredited organizations on the local or State level. A State can address such circumstances through a written exceptions process, and States must document each use of such a process. Exceptions processing is discussed further at section II.F.

5. Signature

DHS proposes that the signature meet the requirements of the existing AAMVA standards for the 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex A, section A.7.7.2. This standard includes requirements for size, scaling, cropping, color, borders, and resolution.

6. Physical Security Features

Section 202(b)(8) of the Act requires that States must include physical security features on driver's licenses and identification cards to ensure they are resistant to tampering, counterfeiting, or duplication for fraudulent purposes. The legislative history of this requirement states:

> The importance of this requirement cannot be overstated. A majority of States maintain a high level of physical security in the manufacture of their cards. Unfortunately, a significant minority of States do not issue licenses or ID cards with secure physical characteristics. This results in criminals, identity thieves, and amateurs such as college students being able to ''manufacture'' fake driver's licenses or ID card from these States. Federal law enforcement officials—national forensic document laboratory—can validate that the driver's license of these States are not secure from counterfeiting using easily available technology.[19]

To develop a regulation that meets these objectives, DHS consulted forensic document experts and evaluated information helpful in determining minimum standards that would achieve significant security benefits within the next few years, make it significantly harder for amateurs to counterfeit or duplicate driver's licenses and identification cards, and enable States to continue to improve the security of their documents.

One option DHS considered was to permit States to select from a ''menu'' of recognized security features contained in many existing driver's licenses and identification cards. This option would essentially continue the status quo and provide States with the most flexibility since no two States would necessarily select the same security feature choices. DHS rejected this option since State choice in this area has not produced sufficiently secure forms of identification. There are a variety of websites offering counterfeit driver's licenses and identification cards from each State, and even trained officers cannot always detect counterfeit identification from another jurisdiction. In addition, this option did not provide sufficient incentives for States to continue to improve the security of their driver's licenses and identification cards.

DHS also considered mandating all the required security features, including the document card stock, to the States. This option had the benefit of producing a set of standardized security features that law enforcement and other personnel could be trained to recognize, would achieve significant security benefits within the next few years, and would make it significantly harder for amateurs to counterfeit or duplicate. States were concerned that a fixed array of features would permit professional counterfeiters to focus on countering a static set of security features and might inhibit States from using new and evolving technology. States were also concerned that mandating the particular card stock a State could use would put States at a competitive disadvantage with potential card stock suppliers and lead to increased costs for the States.

The approach DHS is adopting is to combine some mandatory security features with a performance standard, based on impartial adversarial testing of the card and security features. The mandatory security features DHS proposes, such as the use of offset lithography in place of dye sublimation printing, is designed to impair the ability of amateurs to manufacture counterfeit driver's licenses and identification cards or alter genuine ones. It will also lead to a set of standardized security features that law enforcement and other personnel can be trained to recognize. The use of adversarial testing permits States to experiment with a variety of card stocks and new technologies while fulfilling the underlying security requirements of the Act. DHS understands that a number of different types of card stock,

[18] Title VIII, subtitle C, Sec. 827 (Pub. L. 109–162, 119 Stat. 2960, 3066, Jan. 5, 2006).

[19] H.R. Rep. No. 109–72, at 179 (2005) (Conf Rep.).

including polycarbonate, would likely satisfy the proposed performance standard.

DHS seeks comments on whether the proposed adversarial testing standards will lead to the development of a secure document solution that deters amateurs from producing deceptive counterfeits and/or alterations. DHS also seeks comments on other alternative approaches DHS could pursue on document security to achieve the same objective and how those approaches compare to a performance-based independent adversarial testing. DHS requests that States specifically comment on what contractual issues, if any, the States will face in satisfying the proposed document security requirements if the State's existing license fails one or more of the proposed adversarial tests.

DHS understands that technology is ever-advancing. Therefore, the proposed regulation would establish standards for achieving increased document security for driver's licenses and identification cards. DHS encourages experimentation and development of advanced security technologies.

7. Privacy of the Information Stored on the Driver's License or Identification Card

An important purpose of the Act is to improve law enforcement's ability to confirm the identity of the individual bearing the driver's license or identification card, in order to reduce identity theft and fraud. Authorized users of the information on the REAL ID driver's licenses and identification cards including, but not limited to, law enforcement should be able to access the necessary personal information stored on the driver's license or identification card in order to accomplish a legitimate law enforcement purpose. The ability of commercial entities and other non-law enforcement third parties to collect the personal information encoded on driver's licenses or identification cards raises serious privacy concerns. However, while cognizant of this problem, DHS believes that it would be outside its authority to address this issue within this rulemaking.

As discussed in the Privacy Considerations section of this Preamble, DHS strongly encourages the States to address concerns about the ability of non-law enforcement third parties to collect or skim personal information stored on the REAL ID driver's licenses or identification cards. Some States, such as California, Nebraska, New Hampshire and Texas have passed laws that prohibit the collection of information on a driver's license or identification card. In addition, as noted above, AAMVA has drafted a Model Act [20] that, if enacted by a State, would prohibit commercial users, except as provided by the State's legislation, from using a scanning device to: (1) Obtain personal information printed or encoded on the card and; (2) buy, sell or otherwise obtain and transfer or disclose to any third party or download, use or maintain any data or database, knowing it to contain personal information obtained from a driver's license or identification card. The Model Act authorizes verification of age for purchasing alcoholic beverages or tobacco products, but with strict limitations on the storage and use of such information. DHS supports the privacy and security benefits such State legislation affords and encourages the States to consider the benefits of promulgating the Model Act or similar legislation.

DHS is attempting to achieve a balance between facilitating the ability of law enforcement and other authorized persons to have access to the information on the card and protecting the integrity of the information on the card by limiting the ability of non-authorized persons to obtain that same information. Encryption discussed in section II.H.9 below is one option, but significant concerns exist about the feasibility of deploying encryption, given the need for Federal, State and local law enforcement access.

DHS seeks comments on how best to secure the data, or whether or not to employ protections for the data encoded on the 2D bar code needs to be protected at all, while permitting law enforcement access and what technologies may be available to accomplish this balance. DHS is interested in comments that address whether a technology, such as the National Law Enforcement Telecommunications System (NLETS), or other system currently being used by law enforcement, could be used by the States to provide law enforcement ready access while maintaining the security of the information on the driver's license or identification card.

8. Machine-Readable Technology (MRT)

Section 202(b)(9) of the Act requires the States to include a common MRT with defined minimum data elements for the driver's licenses and identification cards to be accepted by a Federal agency for official purposes. DHS looked at several types of technology that could be used, including:

- A 1D bar code, commonly used for tracking inventory, mostly used by supermarket scanners. This does not have the capability to store significant amounts of information.
- A 2D bar code. This is currently used by 45 of 50 States, plus the District of Columbia. It stores a greater amount of information than the 1D bar code, although the ''scanning'' process is extremely similar to the 1D bar code. This is also the current AAMVA standard.
- An optical stripe. This is currently used on DHS-issued permanent resident cards and border crossing cards, and stores information digitally, much like a compact disc.
- A contact integrated circuit chip. A contact integrated circuit chip (ICC) in a document could be read by inserting the document in a contact ICC reader.
- A contactless integrated circuit chip. A contactless integrated circuit chip in a document could be read by transmitting data via radio frequency to readers.

Of these five options, DHS believes the following are inappropriate for the purposes of this proposal:

- The 1D bar code does not have the storage capacity to hold the amount of data that the Act requires, and would inhibit States from storing additional State-specific information on the card, should they so choose.
- The integrated contactless chip was not deemed an appropriate technology for this particular document, as there is not an identifiable need for driver's licenses and identification cards to be routinely read at a distance.
- The optical stripe has had durability difficulties over time.

Of the two remaining options—the 2D bar code and the contact chip—DHS proposes the 2D bar code as the better option. The 2D bar code is the existing standard for AAMVA, and is also something with which the public is familiar. Forty-five of the fifty United States use this technology currently, making it relatively easy for virtually every State to meet this requirement by May 2008, at little additional cost for most States. The proposed selection of the 2D bar code ensures that the majority of States have available and usable technology that is interoperable among all the States.

The proposed regulation would mandate the use of the PDF–417 2D bar code as the common MRT standard and DHS proposes to adopt most of the mandatory data elements described in the 2005 AAMVA Driver's License/ Identification Card Design

[20] ''Model Act to Prohibit the Capture and Storage of Personal Information Obtained from a Driver's License or ID Card,'' AAMVA 26–8.2–03, 2003.

Specifications, Annex D, as its MRT data elements model. PDF417 is a two dimensional, open source (public domain) barcode that is used to store and transfer large amounts of data inexpensively. PDF stands for ''portable data file'' in that the barcode acts as an independent database that travels along with the item, document, or card on which it is affixed. The printed barcode symbol consists of several linear (minimum 3, maximum 90) rows, each of which is like a small linear barcode made up of code words that can carry up to 1.1 kilobytes of machine-readable data in a space no larger than a standard bar code. The American National Standards Institute has published a standard for PDF417, and AAMVA has approved the use of PDF417 for driver's licenses and identification cards. The PDF417 barcode can be read by a standard 2D barcode scanner.

The AAMVA list of data elements includes expiration date, bearer's name, issue date, date of birth, gender, address, and a unique identification number.[21] DHS proposes that States consider storing in the machine-readable zone (MRZ) only the minimum data elements necessary for the purpose for which the REAL IDs will be used. DHS requests comments on what data elements should be included in the machine readable zone and the privacy considerations regarding the selection of such data elements and this technology.

9. Encryption

Annex D of the AAMVA standard requires that all of the data on the 2D bar code be unencrypted. Although DHS leans toward requiring encryption for the data stored in the 2D bar code on REAL ID driver's licenses and identification cards, DHS believes that access to this information by law enforcement is essential to the requirements of the Act and invites comment on how to provide this access and the protection of the information at the same time.

Because 2D bar code readers are extremely common, there is a possibility that the data could be captured from the driver's licenses and identification cards and accessed by third parties by reading the driver's license or identification card's 2D bar code. For example, a bar could scan the 2D barcode to verify that the individual presenting the driver's license or identification card was 21 or over, and at the same time could conceivably obtain the person's name and address off the barcode and compile a list of names and addresses of its patrons, which it could subsequently sell or use. Encryption would help mitigate this privacy risk by preventing the ''skimming'' of the information from the MRZ, while still allowing the bar to read the date of birth off the face of the license. Alternatively, the date of birth could be left unencrypted so that the bar could scan the date of birth only. Another alternative would be to eliminate the address from the 2D bar code, requiring ''skimmers'' to take the extra step of using information brokers to acquire and match an address to the name and date of birth previously collected off the MRZ.

Because encryption of the data necessitates access to the cryptographic key in order to decrypt the data, employing encryption in the 2D bar code would require having a key infrastructure allowing permitted agencies access to the secured key information. For example, a least 16,000 local, State, and Federal law enforcement agencies would need access to the key infrastructure to check the information on the MRZ.

The need for a key infrastructure to support access to encrypted 2D bar code data could create two separate scenarios of concern.

First, there could be a complex and comprehensive exchange of encryption keys through or among all 56 jurisdictions. Although the encryption system would be most secure the larger the number of keys used to secure MRZ information, this large number of cryptographic keys would need to be accessible to law enforcement personnel wherever they would be reading the driver's license. Building such an infrastructure would present certain complexities that, if not addressed appropriately, could reduce the utility of encryption.

Second, there could be one single encryption key, which would avoid the complexities of needing a key infrastructure, but this greatly increases the risk that this single key could be compromised. Although employing a single key greatly simplifies the availability of the cryptographic key for law enforcement, the compromise of this single cryptographic key would compromise all data secured on all REAL ID driver's licenses and identification cards. In this case, encryption could create a false sense of security if a license holder thought his or her information was truly secure and it was not.

For all of the above reasons, we have not proposed that encryption of MRZ data be required. Nonetheless, DHS leans toward an encryption requirement if the practical concerns identified above can be overcome in a cost-effective manner. We request comments on whether and how encryption could be employed to secure the information stored in the MRZ of the cards.

DHS understands the privacy concerns associated with including personal information in an unencrypted machine readable zone of a driver's license, particularly an individual's address, and also recognizes a legitimate law enforcement need for access to certain data elements. Because of this, DHS seeks comments on whether a demonstrable law enforcement need exists to include address in the MRZ portion of the REAL ID driver's license, as currently proposed in this rule.

I. Validity Period and Renewals of Driver's Licenses and Identification Cards

Section 202(d) of the Act limits the period of validity of all driver's licenses and identification cards that are not temporary to a period that does not exceed eight years.

1. Remote/Non-In-Person Renewals

Under the Act, REAL ID driver's licenses and identification cards (excluding temporary REAL ID driver's licenses and identification cards) may be valid for a period not to exceed eight years. Remote renewal will be allowed for REAL ID driver's licenses and identification cards if the State has retained images or paper copies of the source documents used by the State to issue the original driver's license or identification card through the time of renewal, and if no information has changed since prior issuance (name or address, for example). The State must re-verify information on the source documents that were used as the basis for issuing the original REAL ID driver's license or identification card, to assure there is no match against death information recorded with either the State vital statistics offices or SSA, and in order to diminish the likelihood that an individual obtained his or her original REAL ID driver's license or identification card under a false name or with a fraudulent document.

Finally, under Section 202(d)(4) a State must take reasonable measures to ensure that the individual seeking the renewal is the same person to whom the REAL ID driver's license or identification card was issued. DHS is considering how best to authenticate the identity of an individual requesting renewal of his or her driver's license or identification card remotely, to guarantee that the REAL ID driver's license or identification card is being

[21] The AAMVA standard also includes eye color and height, but DHS is not proposing these as required elements in the machine readable zone.

reissued to its proper holder. For example, DHS proposes that the State may choose to authenticate the identity of a renewal applicant through use of personal identifiers such as PIN numbers or questions whose answers only the proper holder would know, or through use of biometric information. DHS requests comments on these renewal procedures, including suggestions on any alternative approaches for remote renewals and authentication of remote renewals.

2. In-Person Renewals

A holder of a REAL ID driver's license or identification card must renew his or her driver's license or identification card in person with the State DMV at least once every sixteen years (or every other renewal period, if the State chooses a renewal period of less than the eight-year statutory maximum) for the State to take an updated photograph. The States must re-verify original information and source documents used as the basis for issuance of the original REAL ID driver's license or identification card, but the individual need not resubmit documents for verification as long as the State has retained copies of source documents for the period of renewal. Documents supporting name changes or address changes since prior issuance must be presented to the DMV and verified. This process should apply any time a driver's license or identification card is renewed or reissued for any purpose.

Holders of temporary REAL ID driver's licenses and identification cards must renew their driver's licenses and identification cards in person at each renewal in order to present evidence of continued lawful status. States must verify continued lawful status and re-verify source documents as outlined above.

The renewal process for non-REAL ID driver's licenses and identification cards is not subject to this regulation.

J. Source Document Retention

Section 202(d)(1) requires that States employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format. The intent behind this provision is applicant convenience upon renewal, and availability of documentation to law enforcement.[22] DHS is proposing that if a State employs digital imaging of source documents, it use the AAMVA Digital Image Exchange Program for this purpose and capture the image in color. If a State does not currently use color scanners, DHS is proposing that current black and white scanners be replaced with color scanners by December 31, 2011. If a State uses a different standard, that standard must be interoperable with the AAMVA standard to ensure an efficient interstate exchange of data when DMVs need to do so. Photo images should be stored in the Joint Photographic Experts Group (JPEG) 2000 standard for image compression, as modified in the future. Document and signature images should be stored in a compressed Tagged Image Format (TIF). This proposal would require that all images be linked to the applicant through the applicant's unique identifier assigned by the DMV.

As an alternative, a State may retain the paper copies of the source documents until it develops an electronic system.[23] Capturing paper documents on microfiche also would be acceptable, but the State will likely find an electronic system to be more economically efficient over time. Under section 202(d)(2) of the Act, States must retain paper copies of source documents for a minimum of seven years, or images of source documents for a minimum of ten years.

Retaining images of source documents allows for renewal of driver's licenses and identification cards remotely, without requiring the driver's license or identification card holder to present source documents at the renewal. Since REAL ID driver's licenses and identification cards must be issued for a maximum period of eight years in accordance with the Act, States may wish to reconcile their source document retention periods accordingly.

K. Security of DMV Facilities Where Driver's Licenses and Identification Cards Are Manufactured and Produced; Facility Security Plans

DHS is proposing that States that choose to produce REAL ID driver's licenses and identification cards submit to DHS a security plan that outlines the State's consolidated approach to security of DMV facilities and the driver's license or identification card production process. Such security plans should also include the State's approach to conducting background checks of certain DMV employees pursuant to section 202(d)(8) of the Act, physical security of the locations 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, pursuant to section 202(d)(7) of the Act. Security plans should also describe the security features incorporated into the driver's licenses and identification cards as required under section 202(b)(8) of the Act. Also, should the State decide to incorporate biometrics as an additional security feature (which is not mandated in the regulation), DHS is proposing that the State should describe this use in its security plan and present the technology standard the State intends to use to DHS for approval. This will enable DHS to ensure interoperability of technical standards amongst States seeking to incorporate biometrics in their licensing programs.

This proposed regulation would require that the State submit the security plan to DHS in conjunction with the State's request for certification to enable DHS to review the plan, along with the State's request for certification.

1. Background Checks for Certain Employees

Section 202(d)(8) of the Act requires that ''all persons authorized to manufacture or produce driver's licenses and identification cards'' must be required to undergo ''appropriate security clearance requirements.'' The purpose of this requirement is to make sure that those individuals who are in a position to produce, manufacture or issue driver's licenses and identification cards are trustworthy. In some jurisdictions in the past, certain DMV employees involved in this process have aided in the issuance of fraudulent driver's licenses and identification cards.

Section 37.45 of the proposed regulations addresses the requirements of section 202(d)(8) of the Act by identifying which categories of DMV employees must undergo background checks[24] and the nature of the background checks. With respect to scope, Congress made it clear that section 202(d)(8) was included in the Act because recent investigations into driver's license/identification card insider corruption cases in various

[22] H.R. Rep. No. 109–72, at 182 (2005) (Conf. Rep.).

[23] Congress made it very clear in the legislative history of section 202(d)(2) of the Act that the intent is for all States to have an electronic system. ''The goal is to move all the State's records into electronic format.'' H.R. Rep. 109–72, at 182 (2005) (Conf Rep.).

[24] A background check is the investigation into someone's past history to permit them to either gain a security clearance or pass a suitability screening. A security clearance is the end result of a background investigation whereby the government makes a determination that someone may be trusted with specified levels of information, such as ''classified'' information. While section 202(d)(8) of the Act uses the term ''security clearance,'' DHS believes that the intent was to conduct background checks, as DMV employees do not need clearance to handle ''classified'' information.

states ''revealed that a routine security investigation would have prevented key perpetrators from ever being employed to handle documents of high 'street' value that can be sold to illegal aliens, criminals, terrorists, and identity thieves.'' [25]

In light of Congress's clearly expressed intention that background checks be used to prevent the fraudulent creation of identity documents, DHS concluded that background checks should be required for any DMV employee who has the ability to affect the identity information that appears on the driver's license or identification card, who has access to the production process, or who is involved in the manufacture of driver's licenses and identification cards (''covered employees''). Understanding that each State's DMV has a unique organization and structure, it will be up to each State to determine which positions would fall under this definition (''covered positions''). DHS proposes to require that the State DMVs provide their employees and prospective employees that have been selected for placement in a covered position with notice that a background check is required for employment in a covered position and what that background check will include.

With respect to the type of background check required, the regulations propose that States collect fingerprints for individuals who seek employment in a covered position, in order to conduct a criminal history record check (CHRC) on those individuals through the Federal Bureau of Investigation (FBI) and State repositories. Individuals who have been convicted or found not guilty by reason of insanity of certain permanent disqualifying offenses; or individuals who have been convicted or found not guilty by reason of insanity within the previous seven years or who have been released from prison within the past five years for certain interim disqualifying offenses, would not be allowed to hold covered positions within a State DMV. The list of disqualifying offenses, based on current Federal requirements, mirrors requirements for TSA's Hazardous Materials Endorsement program (HAZMAT program) and Transportation Workers Identification Credential (TWIC) program. *See* 49 CFR 1572.103 and the final rule on TWIC (72 FR 3492, Jan. 25, 2007).

DHS concluded that this list of crimes is sufficient as a Federal minimum. States may add additional disqualifying offenses to this list for their covered employees. States will be responsible for arranging reimbursement with the FBI for the cost of conducting the fingerprint CHRC check. DHS invites comment on whether the proposed list of disqualifying offenses is appropriate, too large, or insufficient as it concerns REAL ID.

DHS is also proposing that the States perform a financial history check on individuals seeking employment in covered positions. Such checks are already being conducted by many employers, including many DMVs, as one indicator that an individual may warrant additional scrutiny or supervision before assuming responsibilities that raise security risks. While questionable financial history would not be considered a Federal disqualifier, the information should be used by the States in making their own determinations on how or whether particular individuals should be employed at the DMV.

DHS recognizes that this requirement is not a feature of the TWIC or HAZMAT programs. Nevertheless, DHS believes that it is warranted in the instant case, due to the sensitivity of the personal information that will routinely be handled by employees at State motor vehicle administrations and the fact that a driver's license or identification card serves as a key ''breeder'' document in securing other forms of State and Federal identification. If the DMV personnel issuing and authenticating the driver's license or identification card are compromised and issue genuine REAL ID driver's licenses and identification cards to individuals who are seeking to mask their true identity, those individuals can obtain additional identification using that false identity and thwart the Government's and law enforcement's ability to identify accurately individuals lawfully stopped and screened. Moreover, as set forth in the Conference Report on section 202(d)(8) of the REAL ID Act, Congress was concerned at the extent of ''driver's license insider corruption.'' H.R. Rep. No. 109–72, at 183 (2005) (Conf. Rep.). DHS believes that DMV employees with severe financial difficulties might be more susceptible to bribery, and that States should take this into consideration in determining whether an individual should be placed in a covered position.

These proposed regulations do not preclude a DMV from hiring any individual based on the results of the financial history check and do not preclude the DMV from placing the individual in a covered position based on that check. The financial history check information is intended to provide the employer a fuller picture when deciding whether to place a potential employee in a covered position.

DHS also proposes that States conduct a lawful status check through SAVE to verify that the individual has lawful status in the United States.

DHS proposes that States may grant waivers allowing individuals to maintain their positions under particular circumstances as authorized by the States; for example, where an individual has made full disclosure of his or her criminal history to the State DMV. DHS proposes that States adopt written practices for waiver processes and provide them to DHS as part of the background check discussion of the State's comprehensive security plan. Waiver practices will be reviewed by DHS during a State's initial certification and thereafter as part of periodic DHS audits of the State's REAL ID program.

2. Physical/Logical Security

The Act requires that States ''ensure the physical security of locations 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.'' This means that the DMV buildings, storage areas, databases and systems, and other areas of perceived vulnerability must be protected from theft and fraud. The State's comprehensive security plan should include a written risk assessment of each facility, physical security measures, access identification and control measures for employees and vendors, written policies and procedures, training and internal controls to identify and minimize fraud, and an emergency/incident response plan if procedures are breached.

DHS is considering the American National Standards Institute/North American Security Products Organization's ''Security Assurance Standards for the Document and Product Security Industries,'' ANSI/NASPO–SA–v3.OP–2005, Level II, as the preferred performance-based standard for physical security of DMV facilities. DHS seeks comment on adoption of this standard, as well as recommendations on other appropriate performance-based standards to meet this statutory requirement. DHS also specifically seeks comment on the extent that the adoption of any performance-based standard would require modification of existing office space or construction of new space. DHS also seeks comments on the extent to which physical changes to existing office spaces required by the adoption of

[25] Conference Report at 183.

the ANSI standards or any other physical security performance-based standards would impact historical properties.

3. Document Security Features on Driver's Licenses and Identification Cards

The security plan discussed above must detail the document security features that States are adopting for their driver's licenses and identification cards to prevent tampering, counterfeiting, or duplication of the driver's license or identification card for fraudulent purposes. These features are discussed in more detail in the preamble at Section II.H.6, infra,

4. Security of Information Stored in the DMV Database

Section 202(d)(7) of the Act requires States to ''ensure the physical security of locations 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.'' DHS believes that the scope of this provision includes protecting the security of the personal information stored in DMV databases. The House Conference Report discussion of this section of the Act states that the requirement for improved physical security is to address ''a growing problem of identity thieves and documents purveyors breaking into State facilities and stealing driver's license or identification card stock blanks, printing machines, and sometimes actual computer hard drives in which current driver's license or identification card holder data is stored.'' [26] It is well documented that a number of DMVs have had incidents of theft of personal information from their databases,[27] and security of personal information is a high priority for all Federal and State governmental agencies. Therefore, DHS believes it is reasonable to require that, as part of the security plan mandated for State certification under the Act, States address the security of the DMV databases storing personal information.

5. Security of Personal Data and Documents Collected and Managed Under the Act

As part of the Comprehensive Security Plan, States shall be required to describe standards and procedures for managing driver records and data collected, stored, modified, accessed and transmitted under the requirements of this rule. With respect to the identity documents required to be provided by applicants, States shall describe procedures to prevent unauthorized access to, or dissemination of, images of these documents stored pursuant to the Act. States shall also detail procedures for document retention and destruction for both physical and electronic records. With respect to applicant data required under the Act, States shall document access controls and related procedures governing the authorized use of such data. Finally, States shall document procedures for resolving data formatting, quality, and integrity issues. DHS encourages States to draft collective standards and best practices for the management of both documents and data required under the provisions of this rule.

In the event of a terrorist event or natural disaster as extensive as 9/11 or Hurricane Katrina, the sharing of information collected and maintained by DMVs pursuant to the REAL ID Act may prove useful to the States for many purposes, such a recreating lost State data, providing individuals' access to images of their source documents when originals are destroyed, or assisting in recovery efforts. DHS seeks comment on whether and to what extent States can or should include in their security plans access to data for information sharing purposes as necessary in the event of a catastrophic event.

III. State Certification Process

Section 202(a)(2) of the Act requires the Secretary to determine whether a State is meeting the requirements of the Act based on certifications made by the State to the Secretary of DHS. Certifications ''shall be made at such times and in such manner as the Secretary, in consultation with the Department of Transportation, may prescribe by regulation.'' Section 37.55 of the regulations presents the requirements for certification.

To ease the burden on the States, DHS determined that this certification process should be similar to the certification process included in DOT's regulations governing State administration of commercial driver's licenses, 49 CFR Part 384. The States are accustomed to these certification requirements, and the requirements appear useful in providing the information DHS will need to ensure that States are in compliance with applicable REAL ID standards. Accordingly, Subpart F of these regulations was based, to a large extent, on 49 CFR Part 384. States must demonstrate initial compliance with these regulations by submitting a certification and certain specified documents including a description of its REAL ID program, and demonstrate continued compliance by annually submitting such certification and documents. DHS will review such initial and annual certifications and notify the State of its preliminary determination as to the State's compliance with the regulations. The State will have 30 calendar days to respond to the preliminary determination and explain how any identified deficiencies will be corrected or, alternatively, why the DHS preliminary determination is incorrect. DHS will then notify the State of its final determination for which the State may seek judicial review.

IV. Driver's Licenses and Identification Cards That Do Not Meet the Standards of Subparts A and B of These Regulations

Section 202(d)(11) of the Act requires that any driver's license or identification card that does not satisfy the requirements of this section must clearly state on its face that it may not be accepted by any Federal agency for Federal identification or any other official purpose. DHS is proposing that this statement be in bold lettering on the face of the driver's license or identification card. States must also differentiate non-REAL ID driver's licenses and identification cards from REAL ID driver's licenses and identification cards by incorporating a unique design or color indicator to alert Federal agencies and other law enforcement personnel that it may not be accepted for Federal official purposes pursuant to this regulation. DHS seeks comment on whether a uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards.

V. Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004

Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108–458, 118 Stat. 3638, Dec 17, 2004) requires that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement a plan, as expeditiously as possible, to require travelers entering the United States to present a passport, other document, or combination of documents, that are ''deemed by the Secretary of Homeland Security to be sufficient to denote identity and citizenship.'' Section 7209 of IRTPA is commonly known as the Western Hemisphere Travel Initiative (WHTI).

[26] H.R. Rep. 109–72, at 183 (2005) (Conf. Rep.).

[27] *http://www.cdt.org/testimony/020805schwartz.shtml.*

DHS and DOS issued a final rule on the plan for the air implementation of WHTI which took effect on January 23, 2007. The WHTI requirements for the land and sea borders will be addressed in a separate rulemaking proceeding. In a related WHTI proceeding, DOS issued a Notice of Proposed Rulemaking concerning the Passport Card that would be an acceptable WHTI document at U.S. land and sea borders. See 71 FR 60928 (Oct. 17, 2006). The NPRM proposed that the Passport Card incorporate integrated circuit chip (ICC) technology that would transmit a unique identifier number that could be matched to the holder only in a Government database. The use of ICC technology would facilitate the border inspection of the Passport Card holder. DHS understands that numerous States are interested in exploring whether enhanced driver's licenses and identification cards could be acceptable at the land border to satisfy the WHTI requirements. There are a number of significant differences, however, between a Federally-issued border crossing document and a State-issued driver's license or identification card, including the different vetting criteria. In addition, for purposes of satisfying WHTI requirements, the State would have to ensure that the State-issued REAL ID driver's license or identification card denoted citizenship for purposes of border crossing under WHTI. For REAL ID purposes, DHS is not proposing that States must present the individual's citizenship on the face of the driver's license or identification card or MRZ.

Nevertheless, recognizing the strong interest in some border States to explore the possible interplay between an enhanced driver's license/identification card and WHTI requirements, DHS seeks comments on several topics relating to this notion, including what procedures and business processes a State DMV could develop in order to offer individuals applying for a State-issued REAL ID driver's license or identification card the voluntary option to use the document as a WHTI-compliant border crossing document by meeting some additional requirements. DHS also invites comments on how a State would integrate the type of ICC technology necessary to provide a travel facilitation benefit at the land and sea border along with the common machine readable technology proposed in the REAL ID proceeding while also including an MRZ meeting ICAO standards.

VI. Solicitation of Comments

DHS solicits public comments on all aspects of this proposed regulation. DHS is particularly interested in comments on the following issues:

(1) Whether the list of documents acceptable for establishing identity should be expanded. Commenters who believe the list should be expanded should include reasons for the expansion and how DMVs will be able to verify electronically with issuing agencies the authenticity and validity of these documents.

(2) Whether the data elements currently proposed for inclusion in the machine readable zone of the driver's license or identification card should be reduced or expanded; whether the data in the machine-readable portion of the card should be encrypted for privacy reasons to protect the data from being harvested by third parties, and whether encryption would have any effect on law enforcement's ability to quickly read the data and identify the individual interdicted. What would it cost to build and manage the necessary information technology infrastructure for State and Federal law enforcement agencies to be able to access the information on the machine readable zone if the data were encrypted?

(3) Whether individuals born before 1935 who have established histories with a State should be wholly exempt from the birth certificate verification requirements of this regulation, or whether, as proposed, such cases should be handled under each State's exceptions process.

(4) If a State chooses to produce driver's licenses and identification cards that are WHTI-compliant, whether citizenship could be denoted either on the face or machine-readable portion of the driver's license or identification card, and more generally on the procedures and business processes a State DMV could adopt in order to issue a Real ID driver's license or identification card that also included citizenship information for WHTI compliance. DHS also invites comments on how States would or could incorporate a separate WHTI-compliant technology, such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF417 barcode requirement.

(5) How DHS can tailor the address of principal residence requirement to provide for the security of classes of individuals such as federal judges and law enforcement officers.

(6) What benchmarks are appropriate for measuring progress toward implementing the requirements of this rule and what schedule and resource constraints will impact meeting these benchmarks.

(7) Adoption of a performance standard for the physical security of DMV facility, including whether DHS should adopt the ANSI/NASPO ''Security Assurance Standards for the Document and Product Security Industries,'' ANSI/NASPO–SA–v3.OP–2005, Level II as the preferred standard.

(8) How DHS can better integrate American Samoa and the Commonwealth of the Northern Marianas into the REAL ID framework.

(9) Whether the physical security standards proposed in this rule are the most appropriate approach for deterring the production of counterfeit or fraudulent documents, and what contractual issues, if any, the States will face in satisfying the document security requirements proposed in this rule.

(10) The federalism aspects of the rule, particularly those arising from the background check requirements proposed herein.

(11) How the Federal government can better assist States in verifying information against Federal databases.

(12) In addition to security benefits, what other ancillary benefits could REAL ID reasonably be expected to produce? For example, could REAL ID be expected to reduce instances of underage drinking through use of false/fraudulent identification. If so, please provide details about the expected benefit and how it would be achieved through REAL ID.

(13) The potential environmental impacts of the physical security standards and other requirements proposed under this rule.

(14) Whether other federal activities should be included in the scope of ''official purpose.''

(15) How the REAL ID Act can be leveraged to promote the concept of ''one driver, one record, one record of jurisdiction'' and prevent the issuance of multiple driver's licenses.

(16) Whether DHS should standardize the unique design or color required for non-REAL ID under the REAL ID Act for ease of nationwide recognition, and whether DHS should also implement a standardized design or color for REAL ID licenses.

VII. Regulatory Analyses

A. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that DHS consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA

section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations.

This proposed rule contains new and amended information collection activities subject to the PRA. Accordingly, DHS has submitted the following information requirements to OMB for its review.

Title: Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes.

Summary: This proposal would require States participating in the REAL ID program to meet certain standards in the issuance of driver's licenses and identification cards, including security plans and background checks for certain persons who have the ability to affect the recording of any information required to be verified, or who are involved in the manufacture or production of drivers' licenses and identification cards, or who have the ability to affect the identity information that appears on the license (covered employees).

Use of: This proposal would support the information needs of: (a) The Department of Homeland Security, in its efforts to oversee security measures implemented by States issuing REAL ID driver's licenses and identification cards; and (b) other Federal and State authorities conducting or assisting with necessary background and immigration checks for covered employees.

Respondents (including number of): The likely respondents to this proposed information requirement are States (including the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands) and State agencies (such as Departments of Motor Vehicles) and driver's license and identification card applicants.

Frequency: DHS estimates that each State will submit an initial certification of compliance or request for extension, together with a comprehensive security plan. Subsequently, on an annual basis, each State will re-certify its compliance with the REAL ID Act. States will also submit quarterly reports analyzing their use of the exceptions process and monitoring security trends. Further, DHS anticipates that approximately 17,781 covered employees will receive background checks (Criminal History Records Check or CHRC) on an annual basis. Thus, the annual frequency of information requirements is: 17,781 background checks; 56 annual certifications; and 224 quarterly reports. Background check information will be submitted on an as-needed basis. Additionally, driver's license and identification card applicants must provide proof of identity and lawful status in the U.S. when applying for a REAL ID drivers' licenses or identification cards. Applicants would submit this information only for initial applications or when their lawful status or identifying information has changed.

Annual Burden Estimate: This proposal would result in an annual recordkeeping and reporting burden as follows: States will be responsible for sending initial certifications (including security plans), annual certifications and background check information to the Federal Government. The compilation and transmission of the initial certifications will require an annualized 76,000 labor hours by DMV and/or State government staff. Using an average hourly total cost of compensation of $24.92, the annual burden for labor hours would be $1,895,000.

In the first three years of license issuance, applicants for REAL ID would spend an average of 55.9 million more hours per year. This is equal to approximately 44 additional minutes per applicant on average. This time includes the increase in time to obtain source documents, travel to the DMV, wait in line, and receive service at a customer window.

One-time initial certifications of compliance would require an estimated $1,106,000 for all jurisdictions. Using an average hourly total cost of compensation of $24.92 yields an estimate of 44,397 hours for the first year. This collection occurs only in the first year. However, over three years the annualized burden is 14,799 hours or $368,795.

State annual re-certification would cost the states, on average, $295,035 per year. Using an average hourly total cost of compensation of $24.92 yields an estimate of 11,839 hours each year.

Each quarterly report is likely to require effort similar to the annual re-certifications. Accordingly, the hourly burden estimate is 11,839 hours per quarter or 47,356 hours annually. Using an average total cost of compensation of $24.92 yields a monetized estimate of $1,180,142 per year.

Forwarding information to the Federal Government for the employee background checks would impose an annualized burden of 889 hours on DMVs and/or State governments. This assumes that each submission will take three minutes to forward information for the FBI CHRC. Multiplying the three minutes per transaction by the 17,781 annualized employee background checks yields the annualized hour burden above. Using an average total cost of compensation of $24.92 yields an annual monetized estimate of $22,156.

Driver's license and identification card applicants would incur an annual $171 million in order to seek acceptable source documents as required by this rule.

Running immigration checks on foreign-born applicants for driver's licenses and identification cards will not impart a new hourly burden upon DMVs. DMVs already collect biographic information from applicants' source documentation. At most, this requirement will change which pieces are collected, not the total amount of information collected. Further, the transmission of information to the SAVE system run by DHS will be automated and will therefore not require DMV labor hours to conduct each check.

DHS is soliciting comments to—

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Individuals and organizations may submit comments on the information collection requirements by May 8, 2007. Direct the comments to the address listed in the **ADDRESSES** section of this document, and fax a copy of them to the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: DHS–TSA Desk Officer, at (202) 395–5806. A comment to OMB is most effective if OMB receives it within 30 days of publication. TSA will publish the OMB control number for this information collection in the **Federal Register** after OMB approves it.

As protection provided by the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

B. Economic Impact Analyses

Regulatory Evaluation Summary

Changes to Federal regulations must undergo several economic analyses. A summary of the required analyses follows. A detailed regulatory impact analysis has been prepared as a separate document and is available for review in the docket.

First, Executive Order 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.*, as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. 2531–2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (UMRA, 2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

Although Congress recognized that States will have to expend monies in order to comply with REAL ID,[28] it explicitly stated that the REAL ID Act is binding on the Federal government, and not the States.[29] Moreover, by its terms, UMRA does not apply to regulations ''necessary for the national security'' and those which impose requirements ''specifically set forth in law.'' [30] Thus, as a matter of law, the UMRA requirements do not apply to this proposed rulemaking even though States will be expending resources. However, the analyses that would otherwise be required are similar to those required under Executive Order 12866, which have been completed and may be found in the full Regulatory Evaluation.

[28] *See, e.g.*, section 204(b) authorizing ''such sums as may be necessary to carry out this title.''

[29] *See, e.g.*, section 202(a)(1) (''a Federal Agency may not accept'' no-compliant State licenses) and Conference Report language on section 202(a)(1) (''the law is binding on Federal agencies—not the states'').

[30] *See* 2 U.S.C. 1503(5), 1535.

Executive Order 12866 Assessment

DHS has determined that this rule will have an impact of over $100 million and that it raises novel or complex policy issues. Accordingly, this rule is significant under Section 3(f)(1) of Executive Order 12866 and therefore has been reviewed by the Office of Management and Budget.

DHS has assessed the costs, benefits and alternatives of the requirement proposed under this rule. A complete regulatory impact assessment, as required under Executive Order 12866 and OMB Circular A–4, is set forth in a separate document in the docket for this regulatory action at *http://www.regulations.gov* at Docket Number DHS–2006–0030. A summary of the estimated costs and benefits, including potential ancillary benefits realized by the requirements proposed in this rule, is set forth below.

The Department of Homeland Security (DHS) has conducted a comprehensive, rigorous, and exhaustive Regulatory Evaluation of the benefits and costs of the proposed minimum standards for state-issued driver's licenses and non-driver identification cards pursuant to the REAL ID Act of 2005. Since these standards will impact the lives of approximately 240 million people and the operations of all 56 state and territorial jurisdictions, DHS is committed to an ongoing dialogue with all stakeholders on the benefits and burdens of the proposed regulation. This Regulatory Evaluation is the initial step in joint State, Federal, and public effort to improve the security and trustworthiness of driver's licenses and identification cards.

Assumptions

This Regulatory Evaluation covers the ten-year costs of REAL ID Program deployment and operations. This includes:

- Year One—State and Federal government program startup efforts prior to the statutory deadline of May 2008.
- Years Two through Six—the five-year implementation period ending in May 2013, by which time States must be in full compliance with the statute and regulation
- Years Seven through Ten—four years of program operation

Moreover, this Regulatory Evaluation is based upon five key assumptions and to the extent that any of these five assumptions are relaxed, then it is likely that the compliance costs may be lower.

(1) *That all States will comply with the regulation by the statutory deadline.* DHS recognizes that some States will be unable to comply by May 2008 and will file requests for extensions that may result in phased compliance implementation schedules that could mitigate some of the startup costs examined below. Hence, the costs allocated to the period prior to May 2008—that is, program year one in this analysis—may be redistributed to subsequent years.

(2) *That all Driver's License/Identification (DL/ID) holders will seek a REAL ID credential.* DHS anticipates some individuals may not need to access Federal facilities or fly on commercial airlines or may choose to use a passport or alternative form of photo identification for these purposes. To the extent that some people would not seek a REAL ID credential, then the compliance costs may be considered high.

(3) *That States will issue both REAL IDs and non-REAL IDs.* DHS anticipates that States will offer an alternative DL/ID (not acceptable for Federal official purposes) to those who are unwilling or unable to obtain a compliant one. Thus, this Regulatory Evaluation assumes that States will deploy a two-tier or multi-tier licensing system. States instead may choose to issue only REAL ID compliant driver's licenses and identification cards, thereby reducing their operational and system costs.

(4) *That all IT systems will be functional by the statutory deadline.* DHS has calculated the costs assuming that all required verification data systems be operational and fully populated by May 2008. DHS is working to bring these systems online and up to standards as soon as possible and will work with the States to develop alternative procedures. Again, to the extent that these systems are not operational, then the discounted costs and benefits of the proposed rule may be lower.

(5) *State impact is not uniform due to progress already made in some States.* States that have already invested in improving the security of their licenses will have to invest far less per capita than states with less secure licenses and issuance processes. Those States that are more advanced would incur lower compliance costs than other States.

Costs and Benefits

It is impossible to quantify or monetize the benefits of REAL ID using standard economic accounting techniques. However, though difficult to quantify, everyone understands the benefits of secure and trusted identification. The proposed minimum standards seek to improve the security

and trustworthiness of a key enabler of public and commercial life—state-used driver's licenses and identification cards. As detailed below, these standards will impose additional burdens on individuals, States, and even the Federal government. These costs, however, must be weighed against the intangible but no less real benefits to both public and commercial activities achieved by secure and trustworthy identification.

Economic Costs

The costs of the proposed rule are significant. Implementing the REAL ID Act will impact all 56 State and territorial jurisdictions, more than 240 million applicants for and holders of State DL/IDs, private sector organizations, and Federal government agencies. Figure 1 summarizes the estimated marginal economic costs of the proposed rule over a ten-year period.

FIGURE 1.—ESTIMATED MARGINAL ECONOMIC COST OF REAL ID PROPOSED RULE

Estimated costs (10 years)	$ Million	$ Million (2006 dollars)	% Total	% Total
	7% Discounted	Undiscounted	7% Discounted	Undiscounted
Costs to States	10,770	14,600	62.5	63.2
Customer Services	5,253	6,901	30.5	29.9
Card production	3,979	5,760	23.1	24.9
Data Systems & IT	1,127	1,436	6.5	6.2
Security & Information Awareness	388	471	2.3	2.0
Data Verification	12	18	0.1	0.1
Certification process	10	14	0.1	0.1
Costs to Individuals	5,991	7,875	34.8	34.1
Opportunity Costs (268.8 million hours)	5,401	7,113	31.4	30.8
Application Preparation (161.9 million hours)	3,243	4,283	18.8	18.5
Obtain Birth Certificate (26.5 million hours)	542	700	3.1	3.0
Obtain Social Security Card (15.8 million hours)	302	418	1.8	1.8
DMV visits (64.7 million hours)	1,315	1,712	7.6	7.4
Expenditures: Obtain Birth Certificate	590	762	3.4	3.3
Cost to Private Sector	7	9	0.0	0.0
Costs to Federal Government	451	617	2.6	2.7
Social Security card issuance	349	483	2.0	2.1
Data Verification—SAVE	22	32	0.1	0.1
Data Systems & IT	63	78	0.4	0.3
Certification & training	17	24	0.1	0.1
Total Costs	17,219	23,101	100.0	100.0

Figure 1 shows the primary estimates calculated in both undiscounted 2006 dollars and discounted dollars at a 7% discounted rate. Excluding the cost to individuals, primarily associated with obtaining documents, DHS estimates that the discounted cost of the proposed rule is $11.2 billion ($13.81 per issuance for each of the 813 million issuances over ten years) over ten years. The total discounted cost of the proposed rule, including the cost to individuals is $17.2 billion ($21.18 per issuance). The undiscounted costs are estimated at $15.2 billion ($18.73 per issuance), excluding the direct cost to individuals or $23.1 billion total ($28.41 per issuance). DHS acknowledges that an individual may have more than one application experience over a ten year period due to the expiration period or relocation between states.

States will incur the largest share of the costs as shown in Figure 1. More than 60 percent of the costs (discounted or undiscounted) are associated with providing customer services and card production. Over 30 percent of the costs (discounted or undiscounted) are categorized as costs to individuals and are associated with preparing applications and obtaining necessary documents.

Several factors influence the high cost of this proposed rule. First, this rule is assumed to affect 56 jurisdictions and 240 million license holders. This regulatory evaluation assumes that every license holder will acquire a REAL ID. Second, many individuals will not have their required documents when they need them. Again, the regulatory evaluation realistically assumes that many individuals will need to find the appropriate documents. Third, individuals will need to renew their licenses periodically. DHS does not foresee any way to significantly lessen the 813 million issuances over the next ten years.

Estimated Benefits

The proposed REAL ID regulation would strengthen the security of personal identification. Though difficult to quantify, nearly all people understand the benefits of secure and trusted identification and the economic, social, and personal costs of stolen or fictitious identities. The proposed REAL ID NPRM seeks to improve the security and trustworthiness of a key enabler of public and commercial life—state-issued driver's licenses and identification cards.

The primary benefit of REAL ID is to improve the security and lessen the vulnerability of federal buildings, nuclear facilities, and aircraft to terrorist attack. The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule.

DHS provides a rough ''break-even'' analysis based on the rule having an impact on the annual probability of the U.S. experiencing 9/11 type attacks in the 10 years following the issuance of

the rule.[31] DHS believes that the probability and consequences of a successful terrorist attack cannot be determined for purposes of this benefit analysis. However, for the purposes of this analysis, it is not necessary to assume that there is a probability of being attacked in any particular year. Setting a probability for a successful attack is not necessary for this analysis, so long as we make some admittedly tenuous assumptions about the costs of attack consequences, to determine the reduction in probability of attack that REAL ID would need to bring about so that the expected cost of REAL ID equals its anticipated security benefits. Since it is exceedingly difficult to predict the probability and consequences of a hypothetical terrorist attack, DHS instead provides an answer to the following question: what impact would this rule have to have on the annual probability of experiencing a 9/11 type attack in order for the rule to have positive quantified net benefits. This analysis does not assume that the U.S. will necessarily experience this type of attack, but rather is attempting to provide the best available information to the public on the impacts of the rule. This analysis is preliminary, and DHS specifically requests comments on the methodology used in this discussion, and the types of additional security incidents this rulemaking may impact. DHS is also continuing to develop this analysis for the final rule.

In summary, if these requirements lowered by 3.60% per year the annual probability of a terrorist attack that caused immediate impacts of $63.9 billion (which is an estimate of the immediate impact incurred in the 9/11 attack and might be considered a lower bound estimate), the quantified net benefits of the REAL ID regulation would be positive. If these requirements lowered by 0.61% per year the annual probability of a terrorist attack that caused both immediate and longer run impacts of $374.7 billion (which is an estimate of the immediate and longer run impacts incurred in the 9/11 attack and might be considered an upper bound estimate), the quantified net benefits of the REAL ID regulation would be positive.

The potential ancillary benefits of REAL ID are numerous, as it would be more difficult to fraudulently obtain a legitimate license and would be substantially more costly to create a false license. These other benefits include reducing identity theft, unqualified driving, and fraudulent activities facilitated by less secure driver's licenses such as fraudulent access to government subsidies and welfare programs, illegal immigration, unlawful employment, unlawful access to firearms, voter fraud, and possibly underage drinking and smoking. DHS assumes that REAL ID would bring about changes on the margin that would potentially increase security and reduce illegal behavior. Because the size of the economic costs that REAL ID serves to reduce on the margin are so large, however, a relatively small impact of REAL ID may lead to significant benefits.

Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act of 1980, as amended, (RFA) was enacted by Congress to ensure that small entities (small businesses, small not-for-profit organizations, and small governmental jurisdictions) are not unnecessarily or disproportionately burdened by Federal regulations. The RFA requires agencies to review rules to determine if they have ''a significant economic impact on a substantial number of small entities.'' The following analysis suggests that the proposed rule would not have a significant economic impact on a substantial number of small entities.

Under the RFA, the term ''small entity'' has the same meaning as the terms ''small business,'' ''small organization'' and ''small governmental jurisdiction.'' This action will affect States, and States are governmental jurisdictions. However, States are not considered ''small governmental jurisdictions'' under the RFA. As defined by the RFA, small governmental jurisdictions include governments of cities, counties, towns, townships, villages, school districts, or special districts with a population of less than 50 thousand. The proposed rule would regulate driver's licenses and non-driver identification cards at the state level. It would not directly regulate small government jurisdictions nor would it directly regulate small entities in the driver's license and identification card industry.

The rule would regulate the acceptance of a driver's license or identification card by Federal agencies for official purposes. (If the rule is adopted, Federal agencies would not accept state-issued driver's licenses or identification cards unless they were REAL IDs for the purposes of boarding federally regulated commercial aircraft, entering nuclear power plants and accessing Federal facilities. The rule does not require presentation of this, or any other document, nor does it prohibit the acceptance of any other document.) Consequently, employees and agents would be trained in the acceptance of REAL ID driver's licenses and identification cards to ensure they are compliant with the Act.

The acceptance of REAL ID driver's licenses and identification cards for accessing Federal facilities does not directly regulate small entities as the Federal government is not itself a small entity.

Nuclear power plants qualify as small entities if ''including its affiliates, it is primarily engaged in the generation, transmission, and/or distribution of electric energy for sale and its total electric output for the preceding fiscal year did not exceed 4 million megawatt hours.'' [32] With only three exceptions, every nuclear power plant in the United States produced more than 4 million megawatt hours in fiscal year 2005.[33] However, each of those three plants are owned by companies producing more than 12 million megawatt hours.[34] None of the nuclear power plants qualify as a small business using the SBA definition.

DHS estimates that airlines and their representatives would need to train some of their personnel in the acceptance of REAL ID driver's licenses and identification cards under the proposed rule. While data exist on the number of employees for some firms in the air carrier industry, data do not exist on how many of these employees accept identification from passengers before allowing them to board an aircraft. DHS has therefore established a threshold measure to determine if the proposed regulation would have a significant impact on a substantial number of small entities.

DHS estimates that each employee accepting REAL ID driver's licenses and identification cards for official purposes would require two hours of training. This training will assist personnel in identifying the differences between REAL IDs and non-compliant IDs. The training will also inform personnel about which States are or are not compliant during the phase-in period.

[31] This type of analysis is recommended by OMB Circular A–4 when it is difficult to quantify and monetize the benefits of rulemaking.

[32] Small Business Administration. *Small Business Size Standards Matched to North American Industrial Classification System*, footnote 1. Available at *http://www.sba.gov/size/sizetable2002.html#fn1*. Accessed Jul 14, 2006.

[33] Calculations based on data from the Energy Information Administration. U.S. Department of Energy. *Monthly Nuclear Utility Generation by State and Reactor, 2004 and Monthly Nuclear Utility Generation by State and Reactor, 2005*. Available at *http://www.eia.doe.gov/cneaf/nuclear/page/nuc_generation/gensum.html*. Accessed Jul 14, 2006.

[34] Conclusion based on an internet search conducted on July 14, 2006 of the three specific power plants and the companies that own and operate them.

DHS calculated the fully loaded wage rate of $22.95 per hour for airline ticket counter agents and $22.50 per hour for airport checkpoint staff. Multiplying the wage rates by the estimated two hours to complete the training yields estimates of $45.90 and $45.01 per-employee for ticket counter agents and checkpoint staff, respectively. If a firm's revenue divided by the number of ticket counter agents to be trained is more than $4,590:1 then the effect is less than one percent of their total revenue. To have an impact equal to or greater than three percent of total revenue, the revenue to trained agents would need to be equal to or less than $1,530:1. Firms employing airport checkpoint staff with a total revenue to trained employee ratio greater than $4,501:1 would experience impacts less than one percent of total revenue. DHS estimates that, to have an impact of three percent or more, the firm would need to have a revenue to trained employee ratio equal to, or less than, $1,500:1. DHS is unable to identify any firms for which the total revenue to trained employee ratio would be less than $4,500:1.

Figure 2: IRFA threshold for significant impact

Employee type	Airport ticket counter agent	Airport checkpoint staff
Fully loaded wage	$ 22.95	$ 22.50
Hours of training	2	2
Training cost per employee	$ 45.90	$ 45.01

Impact size (as % of revenue)	Total revenue to trained employee ratio (X : 1)	
1%	$ 4,590	$ 4,501
2%	2,295	2,250
3%	1,530	1,500

This analysis suggests that the proposed rule would not have a significant impact on a substantial number of small entities. The Department welcomes comments and data on the impacts of the proposed regulation on small entities.

International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. There is no international standard for state-issued driver licenses or identification cards. DHS has determined that the proposed regulation would not have an impact on trade.

Unfunded Mandates Assessment

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires Federal agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of more than $100 million in any one year (adjusted for inflation with base year of 1995). Before promulgating a rule for which a written statement is needed, section 205 of the UMRA generally requires agencies to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost-effective, or least burdensome alternative that achieves the objective of the rule. Agencies are also required to seek input from the States in the preparation of such rules.

The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows DHS to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the agency publishes with the final rule an explanation why that alternative was not adopted.

As indicated above, UMRA excludes from its scope regulations which are required for national security reasons. National security was a primary motivator for the REAL ID Act; indeed, the Act itself is an effort to implement recommendations of the 9/11 Commission, and Congress took pains to explain the connection between REAL ID and national security, with over a dozen references to ''terrorists'' or ''terrorism'' in the Conference Report. *See 9/11 Commission Public Report,* Chapter 12.4; Conf. Rep., 179–183.

Notwithstanding the national security nature of the REAL ID Act requirements, DHS has analyzed the estimated cost to states and considered appropriate alternatives to, and benefits derived from, the proposed regulation. Moreover, as detailed in the following section (Executive Order 13132, Federalism), DHS has solicited input from State and local governments in the preparation of this proposed rule.

C. Executive Order 13132, Federalism

Executive Order (E.O.) 13132 requires each Federal agency to develop a process to ensure ''meaningful and timely input by State and local officials in the development of regulatory policies that have federalism implications.'' The phrase ''policies that have federalism implications'' is defined in the Executive Order to include regulations that have ''substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.''

Executive Order 13132 lists as a ''Fundamental Federalism Principle'' that ''[f]ederalism is rooted in the belief that issues that are not national in scope or significance are most appropriately addressed by the level of government closest to the people.'' The issue covered by the instant regulation is, without question, national in scope and significance. It is also one in which the States have significant equities.

While driver's licenses and identification cards are issued by states, they are also the most widely used identification documents. Not

surprisingly, they are very frequently used by Americans to establish their identities in the course of their interactions with the Federal Government (*e.g.*, when entering secure Federal facilities or passing through Federally-regulated security procedures at U.S. airports). The fact that the use of driver's licenses as identity documents is an issue that is ''national in scope'' is illustrated by the events of September 11, 2001. A number of the terrorists who hijacked U.S. aircraft on that day had, through unlawful means, obtained genuine driver's licenses; these documents were used to facilitate the terrorists' operations against the United States.[35]

1. DHS Has Considered the Federalism Implications of Proposed REAL ID Policies

Section 3 of the E.O. sets forth certain ''Federalism Policymaking Criteria.'' In formulating or implementing policies with ''federalism implications,'' agencies are required, to the extent permitted by law, to adhere to certain criteria. DHS has considered this action in light of the criteria set forth in E.O. 13132 section 3(a)–(d) and submits the following:

(a) *Constitutional principles and maximizing the policymaking discretion of the States*. The proposed rule is being promulgated in strict adherence to constitutional principles, and the limits of DHS' constitutional and statutory authority have been carefully considered. DHS is proceeding with this action pursuant to direct Congressional authorization as set forth in the REAL ID Act.

Notwithstanding this clear mandate, DHS has taken steps, in consultation with the States, to maximize policymaking discretion at the state level. In response to concerns expressed during the course of DHS' discussions with stakeholders, DHS has proposed, as part of this rule, an exceptions process (*see* section II.F, *supra*, *Exceptions Processing for Extraordinary Circumstances*) that would allow each State participating in REAL ID to exercise maximum discretion in responding to exigencies arising in the course of verifying an individual's identity.

In section II.K.1 of this proposed rule (section 37.45 of the regulations *Background checks for certain employees*), DHS has recognized that each State's unique situation mandates that the maximum possible latitude be allowed to States in fulfilling the statutory mandate that certain employees undergo background investigations. The proposed rule provides parameters for use by the States in determining which employees are subject to the statutory background check requirements but allows the individual States to make the determinations on a case-by-case basis.

States are also given the discretion to find the best way to determine an individual driver's license or identification card applicant's address of principal residence (*see* sections II.D, II.E.1).

In other aspects of the proposed regulation (*see*, *e.g.*, section II.H.6, *supra*, *Physical Security Features*), DHS has prescribed baseline requirements while allowing States the discretion to impose more stringent standards. Any State that chooses to participate in REAL ID will retain the discretion to issue non-REAL ID driver's licenses and identification cards in any manner it sees fit (provided such driver's licenses and identification cards are clearly identified as non-REAL ID). Most significantly, as set forth above, each State retains the discretion to opt out of REAL ID in its entirety.

(b) *Action limiting the policymaking discretion of the States*. As indicated above, the instant proposed rule strives to maximize State policymaking discretion on two levels: first, because a State's participation in REAL ID is optional; and second, because of the policymaking discretion (*e.g.*, the exceptions process) incorporated into the regulation for States which do choose to participate. DHS believes that it has incorporated into this action the maximum possible State discretion consistent with the purposes of the statute.

(c) *Avoiding intrusive Federal oversight*. Consistent with Congress' vision for REAL ID (*see* section 202(a)(2) of the Act), States which choose to participate in the program will be responsible for monitoring their own compliance. *See* section IV, *State Certification Process*, *supra*. As detailed in that section (and section 37.55 of the instant regulations), the Secretary of Homeland Security will determine whether a State is meeting the requirements of the Act based on certifications made by the State. Certifications ''shall be made at such times and in such manner as the Secretary, in consultation with the Department of Transportation, may prescribe by regulation.''

To facilitate compliance with REAL ID, DHS has adopted a certification process similar to that used by DOT in its regulations governing State administration of commercial driver's licenses. Under the proposed rule, DHS will not directly oversee State compliance. Rather, States will demonstrate initial compliance with REAL ID by submitting a certification and certain specified documents including a description of their REAL ID programs. Continued compliance will be demonstrated through annual submission of such certification and documents. DHS will make compliance determinations based on submissions by the States (and will retain an audit function). States receiving adverse determinations will have the opportunity for an internal appeals process as well as judicial review. Thus, intrusive oversight is avoided by allowing the States themselves to serve as the primary compliance mechanism with this regulation.

(d) *Formulation of policies with federalism implications*. DHS recognizes both the important national interest in secure identity documents and the federalism implications of the policies which underpin this proposed rule. Accordingly, DHS has welcomed and encouraged State participation in this process. Consistent with Congressional intent, DHS has sought, where possible, to draft this regulation in such a way as to maximize State discretion. The examples of exceptions processing and the State certification process are outlined above in this Federalism Statement, and detailed elsewhere in this proposed rule.

Where the exigencies of national security and the need to prevent identity fraud have militated in favor of a uniform national standard (*e.g.*, baseline security features on identity cards and background check requirements), DHS has, as reflected above, consulted with States in order to ensure that the uniform standards prescribed could be attained by the States and would reflect the accumulated security experience of state motor vehicles administrations. The Department recognizes that imposing qualifications for State employees through background check requirements may raise federalism concerns. DHS specifically requests comments on the federalism aspects of the background check requirements proposed under this rule.

2. The REAL ID Proposed Rule Complies With the Regulatory Provisions of E.O. 13132

Under section 6 of E.O. 13132, an agency may not issue a regulation that has federalism implications, that imposes substantial direct compliance costs, and that is not required by statute, unless the Federal Government provides

[35] *See* 9/11 Commission Report, Chapter 12.4.

the funds necessary to pay the direct compliance costs incurred by State and local governments, or consults with state and local officials early in the process of developing the proposed regulation. Moreover, an agency may not issue a regulation that has federalism implications and that preempts State law, unless the Agency consults with State and local officials early in the process of developing the proposed regulation.

(a) *The proposed rule is required by statute.* As stated above, the regulatory requirements of E.O. 13132 apply only to regulations that are not ''required by statute.'' *See* E.O. 13132, section 6(b). The REAL ID Act authorizes the Secretary of Homeland Security to define and implement the various requirements prescribed in the statute; the instant rule merely carries out that mandate. Thus, given the statutory mandate, E.O. 13132's regulatory requirements arguably may not apply to this rulemaking.

(b) *The proposed rule does not preempt state law.* As detailed elsewhere in this document, the REAL ID Act is binding on Federal agencies, rather than on States. The proposed rule would not formally compel any State to issue driver's licenses or identification cards that will be acceptable for federal purposes. Importantly, under this scheme, ''[a]ny burden caused by a State's refusal to regulate will fall on those [citizens who need to acquire and utilize alternative documents for federal purposes], rather than on the State as a sovereign.'' [36] In other words, the citizens of a given State—not Congress—ultimately will decide whether the State complies with this regulation and the underlying statute. DHS has concluded that the proposed rule is consistent with the Tenth Amendment to the U.S. Constitution and does not constitute an impermissible usurpation of state sovereignty. Rather, it is a permissible ''program of cooperative federalism'' in which the federal and state governments have acted voluntarily in tandem to achieve a common policy objective.[37]

(c) *DHS has engaged in extensive consultations with the States.* The statutory mandate and the lack of preemption both satisfy the requirements of E.O. 13132. Nevertheless, in the spirit of federalism, and consistent with section 205(a) of the REAL ID Act, DHS has engaged in extensive consultations with the States prior to issuing this proposed rule. As set forth in section I.B of this proposed rule, DHS held meetings and solicited input from various States and such stakeholders as the National Governors Association and the National Conference of State Legislatures.

In particular, DHS' Office of State and Local Government Coordination hosted three face-to-face meetings (October 2005, January 2006 and February 2006), as well as a conference call (March 2006). DHS also participated in other conferences on REAL ID, hosted by various other stakeholders, including the American Association of Motor Vehicle Administrators. Details of conferences and the input received by DHS from participants are reflected in the docket for this proposed rule and are available for public review as set forth above. *See Reviewing Comments in the Docket, supra.* As detailed in that section, input from the States was instrumental in formulating the policies proposed herein.

(d) *DHS recognizes the burdens inherent in complying with the regulation.* Notwithstanding both the statutory mandate and the Federal (rather than State) focus of the REAL ID Act, DHS recognizes that, as a practical matter, States may view noncompliance with the requirements of REAL ID as an unattractive alternative. DHS also recognizes that compliance with the rule carries with it significant costs and logistical burdens, for which federal funds are generally not available. The costs (to the States, the public and the Federal Government) of implementing this rule are by no means inconsiderable and have been detailed in the regulatory evaluation accompanying this proposed rule.

As indicated above, E.O. 13132 prohibits any agency from implementing a regulation with federalism implications which imposes substantial direct compliance costs on State and local governments unless the regulation is required by statute, the Federal Government will provide funds to pay for the direct costs, or the agency has consulted with State and local officials. In such a case, the agency must also incorporate a federalism statement into the preamble of the regulation and make available to the Office of Management and Budget any written communications from State and local officials. *See* E.O. 13132, section 6(b).

This proposed rule is required by the REAL ID Act. DHS has (as detailed above) consulted extensively with State and local officials in the course of preparing this regulation. Finally, DHS has incorporated this Federalism Statement into the preamble to assess the federalism impact of its proposed REAL ID regulation.

3. REAL ID and Federalism

The issuance of driver's licenses has traditionally been the province of State governments; DHS believes that, to the extent practicable, it should continue as such. However, given the threat to both national security and the economy presented by identity fraud, DHS believes that certain uniform standards should be adopted for the most basic identity document in use in this country. DHS has, in this proposed rule, attempted to balance State prerogatives with the national interests at stake. We look forward to receiving input from States, citizens and other stakeholders with regard to the federalism implications of this proposed rule.

D. Environmental Analysis

Under this proposed rule, DHS is seeking specific public comment and, in particular, information from State DMVs, on the potential environmental impact of the physical standards and other proposed requirements under this rule. DHS will be conducting the necessary analysis to determine the environmental impacts of this rule for purposes of complying with the National Environmental Policy Act of 1969 (NEPA), 42 U.S.C. 4321 *et seq.*, and Council on Environmental Quality (CEQ) regulations, 40 CFR parts 1501–1508, and will be considering public comments received in this analysis.

E. Energy Impact Analysis

The energy impact of the proposed rule has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Pub. L. 94–163, as amended (42 U.S.C. 6362). We have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects in 6 CFR Part 37

Document security, Driver's licenses, Identification cards, Incorporation by reference, Motor vehicle administrations, Physical security.

The Proposed Amendments

For the reasons set forth in the preamble, the Department of Homeland Security proposes to amend 6 CFR chapter I, by adding a new part 37 to read as follows:

[36] *New York* v. *U.S.*, 505 U.S. 144, 173 (1992).

[37] *See* id. at 167.

Title 6—Homeland Security

CHAPTER I—DEPARTMENT OF HOMELAND SECURITY, OFFICE OF THE SECRETARY

PART 37—REAL ID DRIVER'S LICENSES AND IDENTIFICATION CARDS

Subpart A—General

Subpart B—Minimum Documentation, Verification and Driver's License and Identification Card Issuance Requirements

Subpart C—Other Requirements

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

Subpart E—Procedures for Determining State Compliance

Subpart F—Non-REAL ID Driver's Licenses and Identification Cards

Authority: 49 U.S.C. 30301 note; 6 U.S.C. 111, 112.

Subpart A—General

§ 37.1 Applicability.

(a) Subparts A through F of this part apply to States and territories that choose to issue driver's licenses and identification cards that can be accepted by Federal agencies for official purposes.

(b) Subpart F of this part establishes certain standards for State-issued driver's licenses and identification cards that do not meet the standards for acceptance for Federal official purposes.

§ 37.3 Definitions.

For purposes of this part:

Birth certificate means the record related to a birth that is permanently stored either electronically or physically at the State Office of Vital Statistics or equivalent agency in a registrant's State of birth.

Card means either a driver's license or identification card issued by the State DMV or equivalent State office.

Certification means an assertion by the State that the State has met the requirements of this part.

Certified copy of a birth certificate means a copy of the whole or part of a birth certificate registered with the State that the State considers to be the same as the original birth certificate on file with the State Office of Vital Statistics or equivalent agency.

Covered employees means DMV employees or DMV contractors who have the ability to affect the recording of any information required to be verified, or who are involved in the manufacture or production of 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.

Data verification means checking the data contained in source documents presented under this regulation against authoritative reference databases.

Department of Motor Vehicles means any State Government entity that issues driver's licenses and identification cards, or an office with equivalent function for issuing driver's licenses and identification cards.

Determination means a decision by the Department of Homeland Security that a State has or has not met the requirements of this part and that Federal agencies may or may not accept the driver's licenses and identification cards issued by the State for official purposes.

DHS means the U.S. Department of Homeland Security. When used in connection with the issuance of documents, the term also includes the former Immigration and Naturalization Service (INS) of the Department of Justice when INS issued documents that are still valid.

Digital photograph means a digitally printed reproduction of the face of the holder of the license or identification card.

Document authentication means verifying that the source document presented under these regulations is genuine and has not been altered.

Domestic violence and dating violence have the meanings given the terms in section 3, Universal definitions and grant provisions, of the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109–162, 119 Stat. 2960, 2964, Jan. 5, 2006); codified at section 40002, Definitions and grant provisions, 42 U.S.C 13925.

Driver's license means a motor vehicle operator's license, as defined in 49 U.S.C. 30301.

Federal agency means all executive agencies including Executive departments, a Government corporation, and an independent establishment as defined in 5 U.S.C. 105.

Federally-regulated commercial aircraft means a commercial aircraft regulated by the Transportation Security Administration (TSA).

Full legal name means an individual's first name, middle names or family names, and last name, without use of initials or nicknames.

IAFIS means the Integrated Automated Fingerprint Identification System, a national fingerprint and criminal history system maintained by the FBI that provides automated fingerprint search capabilities.

Identification card means a document made or issued by or under the authority of a State Department of Motor Vehicles which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.

Lawful status: A person in lawful status: is a citizen or national of the United States; Is an alien lawfully admitted for permanent or temporary residence in the United States; has conditional permanent resident status in the United States; has an approved application for asylum in the United States or has entered into the United States in refugee status; has a valid nonimmigrant status in the United States; has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for LPR or conditional permanent resident status.

NCIC means the National Crime Information Center, a computerized index of criminal justice information maintained by the FBI that is available to Federal, state, and local law enforcement and other criminal justice agencies.

Official purpose means accessing Federal facilities, boarding Federally-regulated commercial aircraft, and entering nuclear power plants.

Passport means a passport booklet or card issued by the Department of State that can be used as a travel document to gain entry into the United States and that denotes identity and citizenship as determined by the Department of State.

Principal residence means where a person has his or her true, fixed, and permanent home and to where he or she has the intention of returning whenever he or she is absent.

REAL ID Driver's License or Identification Card means a driver's license or identification card that meets the standards of subparts A through D of this part, including temporary driver's licenses or identification cards issued under § 37.21.

Reissued means a card that a State DMV issues to replace a card that has been lost, stolen or damaged.

SAVE means the DHS Systematic Alien Verification for Entitlements system, or such successor or alternate verification system at the Secretary's discretion.

Secretary means the Secretary of Homeland Security.

Sexual assault and stalking have the meanings given the terms in section 3, Universal definitions and grant provisions, of the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109–162, 119 Stat. 2960, 2964, Jan. 5, 2006); codified at section 40002, Definitions and grant provisions, 42 U.S.C 13925.

Source document(s) means original or certified copies (where applicable) of documents presented by an applicant as required under these regulations to the Department of Motor Vehicles to apply for a driver's license or identification card.

Source information means the pertinent information present on source documents that are presented by an applicant to the Departments of Motor Vehicles to apply for a driver's license or identification card.

State means a State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

State address confidentiality program means any State-authorized or State-administered program that—

(1) Allows victims of domestic violence, dating violence, sexual assault, stalking, or a severe form of trafficking to keep, obtain, and use alternative addresses; or

(2) Provides confidential record-keeping regarding the addresses of such victims.

Temporary lawful status: A person in temporary lawful status is a person who: Has a valid nonimmigrant status in the United States; has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for LPR or conditional permanent resident status.

§ 37.5 Deadlines and validity periods for REAL ID driver's licenses and identification cards.

(a) *Cards issued on or after May 11, 2008.* A State-issued driver's license or identification card issued on or after May 11, 2008 is acceptable by Federal agencies for official purposes only if the card meets the requirements of this part, and DHS has determined that the issuing State meets the requirements of the REAL ID Act of 2005 (Pub. L. 109–13, 119 Stat. 231, 302, May 11, 2005).

(b) *Cards issued before May 11, 2008.* If DHS determines that a State is in compliance with the REAL ID requirements in this part, all cards issued before May 11, 2008 are acceptable by Federal agencies for official purposes until and including May 10, 2013. All cards issued, reissued, or renewed after May 11, 2008 must be REAL ID compliant by May 11, 2013 or they shall not be acceptable by Federal agencies for official purposes.

(c) *REAL ID card validity period.* Driver's licenses and identification cards issued under this part that are not temporary driver's licenses and identification cards are valid for a period not to exceed eight years. A card may be valid for a shorter time period based on other State or Federal requirements.

Subpart B—Minimum Documentation, Verification, and Card Issuance Requirements

§ 37.11 Application and documents the applicant must provide.

States must require each individual applying for a REAL ID driver's license or identification card to have their photograph taken by the DMV, and maintain that photograph as described in paragraph (a) of this section. States must further require each individual applying for a REAL ID driver's license or identification card to submit the declaration in paragraph (b) and to present the documents described in paragraphs (c), (d), (e) and (f) of this section. Documents in paragraph (g) of this section are required as described in that paragraph. States are not required to comply with these requirements when issuing REAL ID driver's licenses or identification cards in support of Federal, State, or local criminal justice agencies or programs that require special licensing or identification to safeguard persons or in support of their other official duties. As directed by appropriate officials of these Federal, State, or local agencies, States should take sufficient steps to safeguard the identities of such persons. Driver's licenses and identification cards issued in support of Federal, State, or local criminal justice agencies or programs that require special licensing or identification to safeguard persons or in support of their other official duties shall not be distinguishable from other REAL ID licenses or identification cards issued by the State.

(a) The State must subject each person applying for a REAL ID driver's license or identification card to a mandatory facial image capture, whether or not such person is issued a REAL ID driver's license or identification card. Photographs of individuals who were not issued a REAL ID driver's license or identification card must be kept for 1 year, unless the DMV did not issue the driver's license or identification card because of suspected fraud, in which case the record should be maintained for ten years and reflect that a driver's license or identification card was not issued for that reason.

(b) *Declaration.* Each applicant must sign a declaration under penalty of perjury that the information presented is true and correct, and the State must retain this declaration with copies of the applicant's source documents pursuant to § 37.31. An applicant must sign a new declaration when presenting new information to the DMV.

(c) *Identity.* (1) To establish the individual's identity, the individual must present at least one of the following documents containing a photograph or non-photo identity document including full name and date of birth:

(i) A valid unexpired United States passport.

(ii) Certified copy of a birth certificate issued by a U.S. State or local office of Public Health, Vital Records, Vital Statistics or equivalent office.

(iii) Consular Report of Birth Abroad issued by DOS, Form FS–240, DS–1350 or FS–545.

(iv) An unexpired Permanent Resident Card issued by DHS, Form I–551.

(v) An unexpired employment authorization document (EAD) issued by DHS, Form I–766 or Form I–688B.

(vi) Unexpired foreign passport with a valid unexpired U.S. visa affixed.

(vii) Certificate of Naturalization issued by DHS, Form N–550 or Form N–570.

(viii) Certificate of Citizenship, Form N–560 or Form N–561.

(ix) REAL ID driver's license or identification card issued in compliance with the standards established by this part.

(2) If the individual's name has changed through adoption, marriage, divorce, or court order, the individual must present an original or certified copy of the documents showing a legal name change, before the name is changed on the driver's license or identification card. These documents must come from a U.S. or State-level Court or government agency.

(d) *Date of birth.* To establish the person's date of birth, the individual must present at least one document included in paragraph (c) of this section.

(e) *Social security number.* The individual must provide documentation establishing an SSN, or the person's ineligibility for an SSN.

(1) To establish an SSN, an applicant must present his or her social security account number card, a W–2 form, a SSA–1099 form, a non-SSA 1099 form, or a pay stub with the applicant's name and SSN on it; the SSN must be verified pursuant to § 37.13 of this subpart.

(2) To establish ineligibility for an SSN, an alien must present evidence that he or she is currently in a non-work authorized nonimmigrant status.

(f) *Documents demonstrating address of principal residence.* To document the address of principal residence, a person must present at least two documents of the State's choice that include the individual's name and principal residence.

(1) Documents used to demonstrate address of principal residence that are issued monthly (such as bank statements or utility bills) must not be more than three months old at the time of application.

(2) Documents used to demonstrate address of principal residence that are issued annually (such as property tax records) must be for the most current yearly period at the time of application.

(3) Except as provided in § 37.17(f)(1), (f)(2) and (f)(3) of this part, a street address must be required.

(g) *Evidence of lawful status in the United States.* A DMV may issue a REAL ID driver's license or identification card only to a person who has presented satisfactory evidence of lawful status. The documentation listed under paragraph (c) of this section is also evidence of lawful status, except that if the applicant presents an identity document listed under paragraphs (c)(1)(v) or (c)(1)(vi) of this section, the documentation is to be considered provisional evidence pending verification of immigration status through SAVE. If the applicant presents an identity document listed under paragraph (c)(1)(ix) of this section, he or she must also present another document listed in paragraph (c) of this section as evidence of lawful presence in the United States.

(h) State DMVs may choose to establish a written exceptions process in order to provide REAL ID driver's licenses and identification cards to persons who, for reasons beyond their control, are unable to present all necessary documents and must rely on alternate documents to establish identity. An exceptions process may not be used to demonstrate lawful status. Each State establishing an exceptions process must have that process approved by DHS for the verification of documents in this section, and document each time the process is used, both on the applicant's record in the DMV's database and in the DMV's files.

(1) The applicant's records must visibly indicate when an alternate document is accepted and how applicable information from the document was verified.

(2) The record must include a full explanation of the reason for the exception and alternative documents accepted whenever a driver's license or identification card is issued using exceptions processing.

(3) The State shall retain copies of the alternate documents accepted pursuant to this section and provide these upon request to DHS for audit.

(4) The State shall provide DHS with quarterly reports analyzing the use of the exceptions process and any trends that indicate potential vulnerabilities.

§ 37.13 Document verification requirements.

States must adopt procedures satisfying the requirements of paragraph (a) of this section to verify with the issuing agency the issuance, validity, and completeness of a document presented to demonstrate a person's eligibility for a REAL ID driver's license or identification card before issuance of the driver's license or identification card.

(a) States must use the following procedures to verify the documents required under this section:

(1) A certified copy of a birth certificate must be verified through the Electronic Verification of Vital Events System, or an alternative approved by DHS. In the event of a non-match, the DMV may not issue a driver's license or identification card to an applicant, and must refer the individual to their birth state's vital statistics office for resolution.

(2) A U.S. passport or Consular report of birth abroad must be verified through existing Department of State systems.

(3) A lawful permanent resident card (Form I–551) or other DHS-issued document demonstrating permanent residency, an EAD (Form I–766 or Form I–688B), Certificate of Citizenship, Certificate of Naturalization, or other documentation issued by DHS demonstrating lawful status, must be verified through the Systematic Alien Verification for Entitlements (SAVE) system operated by DHS, or an alternate verification system approved by DHS. In the event of a non-match to SAVE, the DMV may not issue a driver's license or identification card to an applicant, and must refer the individual to the local USCIS office for resolution.

(4) REAL ID driver's licenses and identification cards must be verified with the State of issuance.

(5) Social security account numbers must be verified by the Social Security Administration's (SSA) electronic database. In the event of a non-match with SSA, a DMV must not issue a driver's license or identification card to an applicant until the information verifies with SSA's database.

(6) Documents demonstrating address of principal residence must be verified by the State in accordance with a system of document verification acceptable to DHS, to ensure that a document produced establishes an individual's address of principal residence.

§ 37.15 Physical security features for the driver's license or identification card.

(a) *General.* States must include document security features on REAL ID driver's licenses and identification cards designed to deter forgery and counterfeiting and promote an adequate level of confidence in the authentication of genuine documents and the detection of fraudulent ones in accordance with this section.

(1) These features must not be reproducible using commonly used or available technologies.

(2) The proposed card solution must contain a well designed, balanced set of features that when effectively combined provide multiple layers of security. States must describe these document security features in their security plans pursuant to § 37.41.

(b) *Integrated security features.* REAL ID driver's licenses and identification cards must contain at least three levels

of integrated security features that provide the maximum resistance to persons' efforts to—

(1) Counterfeiting, simulating, or reproducing a genuine document;

(2) Altering, deleting, modifying, masking, or tampering with data concerning the original or lawful card holder;

(3) Substituting or altering the original or lawful card holder's photograph and/or signature by any means; and

(4) Creating a fraudulent document using components from legitimate driver's licenses or identification cards.

(c) *Security features to detect false cards.* States must employ security features to detect false cards for each of the following three levels:

(1) *Level 1.* Cursory examination, without tools or aids involving easily identifiable visual or tactile features, for rapid inspection at point of usage.

(2) *Level 2.* Examination by trained inspectors with simple equipment.

(3) *Level 3.* Inspection by forensic specialists.

(d) *Minimum security features.* States must employ, at a minimum, the following security features in each REAL ID driver's license or identification card:

(1) An intricate, fine-line, multicolored background design produced via offset lithography that includes microcline printing and an intentional error/field check.

(2) An optically variable feature providing adequate protection against copying. The inclusion of a diffractive optically variable feature is recommended to achieve an enhanced level of protection.

(3) An ultraviolet (UV) long wave responsive feature.

(4) The proposed card solution must include cards constructed such that application of personal data provides for the highest quality of printed information including sufficient depth, clarity and resolution. The application of variable data shall be in a manner that is considered secure and difficult, if not virtually impossible, to erase, modify or otherwise successfully tamper. Some variable data must be applied via laser engraving to include tactile features (that protect the bearer portrait from substitution via thin film overlay) and variable microline text that is specific to the bearer. The laser must effectively penetrate the card layers ensuring that the data is engraved into the layers containing the security characteristics.

(5) A series of check digit numbers or letters printed on the cards.

(6) Incorporation of covert taggants and/or markers.

(e) *Document card stock.* States must use a document card stock in the issuance of REAL ID driver's licenses and identification cards that complies with the following performance standards:

(1) The card stock must be UV dull or possess a controlled response to UV, such that when illuminated by UV light it exhibits fluorescence distinguishable in color from the blue used in commonly available fluorescent materials. The card stock must use suitable materials that provide for a highly durable card stock that can survive, at least, an eight-year card life. If the card stock is a multi-layered structure, there must be adequate adhesion and/or tamper evident properties to protect the personalized data and security features contained in the card. The card stock must provide for the highest clarity for information applied.

(2) External surfaces of the cards must be printed using recognized security printing methods to resist duplication or facsimile reproduction by commercially available products. The card must bear a security background pattern designed to be resistant to counterfeiting by scanning, printing or copying. To achieve this, the background pattern shall not be composed of the primary colors Cyan, Magenta, Yellow and Key (Black) (CMYK). The pattern shall show no evidence of half-tone dots, or pixel structure typically found in digital printing technologies.

(3) States must issue REAL ID driver's licenses and identification cards produced on serialized card stock and implement controlled inventory measures that meet recognized industry standards. The State must maintain a record of any missing cards and report the loss to the DMV and to law enforcement.

(4) Driver's licenses and identification cards must contain a revision date that is printed or engraved on the card surface and which must be updated whenever the card design changes.

(5) States must provide DHS with samples of REAL ID driver's licenses and identification cards in a quantity that DHS will specify. The cards provided will be representative of issued driver's licenses and identification cards, produced on equipment identical to that used by the State to issue REAL ID driver's licenses and identification cards, and include all data fields and security features used by the State.

(f) *Document security and integrity.* (1) States must conduct an annual review of their card design and submit a report to DHS that indicates the ability of the designs to resist compromise and document fraud activity attempts. The report must be submitted as part of the State's annual certification. The report required by this paragraph is Sensitive Security Information (SSI) and will be handled in a manner consistent with DHS regulations concerning SSI published at 49 CFR part 1520.

(i) States must provide DHS with examination results from a recognized independent laboratory experienced with adversarial analysis of identification documents as part of the State's initial certification under § 37.55, and annual certification under § 37.57.

(ii) As part of the State's initial and annual certifications, the State must submit to DHS results from a facility described in paragraph (g)(2)(i) of this section, in the following areas:

(A) Photo substitution.

(B) Delamination and deconstruction.

(C) Reverse engineering.

(D) Modification of any data element.

(E) Erasure of information.

(F) Duplication, reproduction, or facsimile creation.

(G) Effectiveness of security features (three levels).

(H) Confidence and ease of second level authentication.

(iii) The specifics of the lab analysis requirements and the analysis results are Sensitive Security Information (SSI) and will be handled in a manner consistent with DHS regulations concerning SSI at 49 CFR part 1520.

(iv) DHS may change lab analysis requirements under this section upon notice to the State and opportunity for comment or immediately if DHS determines that there is a need for immediate application of the new requirements.

§ 37.17 Requirements for the face of the driver's license or identification card.

To be acceptable by a Federal agency for official purposes, REAL ID driver's licenses and identification cards must include on the face of the card the following information:

(a) *Full legal name.* The name on the face of the card must be the same as the name on the document presented by the applicant to establish identity. This includes the individual's first name, middle names or family names, and last name without use of initials or nicknames.

(b) *Date of birth.*

(c) *Gender.*

(d) *Unique Driver's license or identification card number.* This cannot be the individual's Social Security Number (SSN).

(e) *Full facial digital photograph.* A full facial photograph must be taken pursuant the standards set forth below:

(1) Lighting shall be equally distributed on the face.

(2) The face from crown to the base of the chin, and from ear-to-ear, shall be clearly visible and free of shadows. States use photographs in profile rather than ear-to-ear to differentiate licensees that are under the age of 21.

(3) Veils, scarves or headdresses must not obscure any facial features and not generate shadow. The person may not wear eyewear that obstructs the iris or pupil of the eyes.

(4) There must be no dark shadows in the eye-sockets due to the brow. The iris and pupil of the eyes shall be clearly visible.

(5) Care shall be taken to avoid ''hot spots'' (bright areas of light shining on the face).

(f) *Address of principal residence*, except individuals who satisfy one of the following:

(1) If the individual is enrolled in a State address confidentiality program;

(2) If the individual's address is entitled to be suppressed under State or Federal law or suppressed by a court order; or

(3) If the individual is protected from disclosure of information pursuant to section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

(g) *Printed information.* The name, date of birth, gender, card number, issue date, expiration date, and address on the face of the card must be in Roman alphabet characters. The name must contain a field of no less than a total of 39 characters for the full legal name, and longer names may be truncated following the standard established by International Civil Aviation Organization (ICAO) 9303, ''Machine Readable Travel Documents,'' Part IV, Sixth Edition, 2005. The Director of the Federal Register approves this incorporation by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of ICAO 9303 from the ICAO, Document Sales Unit, 999 University Street, Montréal, Quebec, Canada H3C 5H7, tel: 1–(514) 954–8022; E-mail: *sales@icao.int.* You may inspect a copy at the Office of the Federal Register, 800 N. Capitol Street, NW., Suite 700, Washington, DC.

(h) *Signature.* The card must include the signature of the card holder. The signature must meet the requirements of the existing American Association of Motor Vehicle Administrators (AAMVA) standards for the 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex A, section A.7.7.2. This standard includes requirements for size, scaling, cropping, color, borders, and resolution. The Director of the Federal Register approves this incorporation by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of these standards from AAMVA on-line at *http://www.aamva.org*, or by contacting AAMVA at 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203, tel. (703) 522–4200. You may inspect a copy at the Office of the Federal Register, 800 N. Capitol Street, NW., Suite 700, Washington, DC.

(i) *Physical security features*, pursuant to § 37.15 of this subpart.

(j) *Machine-readable technology*, pursuant to § 37.19 of this subpart.

(k) *Issuance date.*

(l) *Expiration date.*

§ 37.19 Machine readable technology on the driver's license or identification card.

For the machine readable portion of the REAL ID driver's license or identification card, States must use PDF417 2D bar code standard, with the following defined minimum data elements:

(a) Expiration date.

(b) Holder's name. The machine readable portion of the card must have at least 125 characters to permit capture of the full name history, including full legal name and all name changes.

(c) Issue date.

(d) Date of birth.

(e) Gender.

(f) Address.

(g) Unique identification number.

(h) Revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card.

(i) Inventory control number of the physical document.

§ 37.21 Temporary driver's licenses and identification cards.

States may issue only a temporary driver's license or identification card to an individual who has temporary lawful status in the United States.

(a) States must require, before issuing a temporary driver's license or identification card to a person, valid documentary evidence that the person has lawful status in the United States, as determined by DHS, and verification of that status through SAVE.

(b) States shall not issue a temporary driver's license or identification card pursuant to this section:

(1) For a time period longer than the expiration of the applicant's authorized stay in the United States, or, if there is no expiration date, for a period longer than one year.

(2) For longer than eight years or the State's maximum driver's license or identification card term.

(c) States shall renew a temporary driver's license or identification card pursuant to this section and § 37.23(b)(2), only if:

(1) The individual presents valid documentary evidence that the status by which the applicant qualified for the temporary driver's license or identification card has been extended by DHS, or

(2) The individual presents valid documentary evidence that they have qualified for another lawful status under paragraph (a) of this section, and such continued or new status is verified through SAVE.

(d) States must verify the documents an individual presents to establish his or her temporary lawful status through SAVE.

(e) Temporary driver's licenses and identification cards must clearly state on the face of the driver's license or identification card in bold lettering, and in the machine readable zone of the driver's license or identification card, that it is temporary.

§ 37.23 Renewed and reissued driver's licenses and identification cards.

(a) *General.* Any driver's license or identification card that is renewed or reissued between May 11, 2008, and May 10, 2013 that is intended to be acceptable by federal agencies for official purposes must meet the standards set forth in subparts A through C of this part.

(b) *State procedure.* States must establish an effective procedure to confirm or verify an applicant's identity each time a REAL ID driver's license or identification card is renewed or reissued, to ensure that the individual receiving the renewed or reissued REAL ID driver's license or identification card is the same individual to whom the driver's license or identification card was issued originally.

(1) *Remote/Non-in-person renewals and reissuance.* Except as provided in paragraph (b)(2) of this section a State may conduct a non-in-person (remote) renewal or reissuance if the State continues to retain the images or copies of source documents presented by the individual and used by the State to issue the REAL ID driver's license or identification card, and no source information has changed since prior issuance.

(i) The State must re-verify information from the images or copies of the source documents used as the basis for issuance of the original REAL ID driver's license or identification card at each renewal and reissuance in accordance with § 37.13 of this part.

(ii) Any information that has changed since prior issuance (such as name or address) must be established through presentation of an original source document as provided in Subpart B, and must be verified, or, in the case of address, validated.

(iii) The process described in paragraph (b) of this section applies any time a driver's license or identification card is renewed or reissued for any purpose.

(2) *In-person renewals.* States must require holders of REAL ID driver's licenses and identification cards to renew their driver's licenses and identification cards with the State DMV in person, every other renewal cycle, or at least once every 16 years.

(i) The State shall take an updated photograph of the applicant, at least at every other renewal.

(ii) The States must re-verify information and source documents used as the basis for issuance of the original REAL ID driver's license or identification card, or must require the individual to resubmit documents and verify those documents.

(iii) Holders of temporary REAL ID driver's licenses and identification cards must renew their driver's license or identification card in person each time, and present evidence of continued lawful status.

Subpart C—Other Requirements

§ 37.31 Source document retention.

States must retain copies of the application, declaration and source documents presented under § 37.11 of this part.

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

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

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

(1) States currently using black and white imagers must replace them with color imagers by December 31, 2011.

(2) States using digital imaging to retain source documents, must use the AAMVA Digital Image Exchange Program, or a standard other than AAMVA that has interoperability with the AAMVA standard, so that the digital images are retained in electronic storage in a transferable format.

(i) 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.

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

(iii) All images must be linked to the applicant through the applicant's unique identifier assigned by the DMV.

§ 37.33 Database connectivity with other States.

(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 Social Security Number; and

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

(b) States must provide to all other States electronic access to information contained in the motor vehicle database of the State, in a manner approved by DHS pursuant to this regulation. This section does not intend to supersede DOT requirements codified at 49 CFR parts 383 and 384.

(c) Prior to issuing a REAL ID driver's license or identification card, States must check with all other States to determine if any State has already issued a REAL ID driver's license or identification card to the applicant.

(1) If the State receives confirmation that the individual currently holds a REAL ID driver's license or identification card issued by another State, the receiving State must:

(i) Take measures to confirm that the person has taken steps to terminate, or has terminated, the REAL ID driver's license or identification card issued by the prior State.

(ii) Require the person to surrender the REAL ID driver's license or identification card issued by another State, unless the person signs a declaration under penalty of perjury pursuant to 28 U.S.C. 1746 stating that the driver's license or identification card was lost or stolen.

(iii) If the person signs a declaration stating that the driver's license or identification card was lost or stolen in another State, the State receiving the declaration must inform the State that issued the driver's license or identification card that it has been reported as lost or stolen.

(iv) The State that issued the driver's license or identification card reported as lost or stolen must record that information on its database and terminate that driver's license or identification card upon notice from another State.

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

§ 37.41 Comprehensive security plan.

(a) States must prepare a comprehensive security plan for all State DMV offices and driver's license/identification card storage and production facilities, and submit it as part of its application for certification.

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

(1) Physical security for the following:

(i) Buildings used to manufacture or issue driver's licenses and identification cards.

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

(iii) Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the physical location and the personal information stored and maintained in DMV records and information systems.

(2) Document and physical security features for the face of 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;

(3) Access control, including the following:

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

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

(iii) Controlled access systems.

(4) Periodic training requirements in—

(i) Fraudulent document recognition, approved by DHS, for appropriate employees engaged in the issuance of driver's licenses and identification cards.

(ii) Domain awareness training including threat identification;

(5) Privacy policy regarding personal information collected and maintained by the DMV;

(6) Emergency/incident response plan;

(7) Internal audit controls;

(8) The State's standards and procedures for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including 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;

(9) Procedures to revoke and confiscate driver's licenses or identification cards fraudulently issued in another State;

(10) 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 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 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; and

(11) Other information as determined by DHS.

§ 37.43 Physical security of DMV facilities.

(a) States must ensure the physical security of locations 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. State compliance with a performance-based standard approved by DHS will satisfy this requirement.

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

§ 37.45 Background checks for covered employees.

(a) *Scope.* States are required to subject persons who have the ability to affect the recording of any information required to be verified, or 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 (covered employees), 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, a financial history check, and a lawful status check. States shall describe their background check process as part of their comprehensive security plan, in accordance with § 37.41. This section also applies to contractors utilized in covered positions under this paragraph.

(b) *Background checks.* States must ensure that any covered employee or prospective 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, before employment in a covered position commences. For persons employed in covered positions on the effective date of this regulation, States must complete the background check described in this section prior to that person's participation in the issuance of any REAL ID driver's licenses or identification cards that comply with this part.

(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 NCIC and IAFIS database and State repository records on each covered employee or prospective employee identified in paragraph (a) of this section, and determine if the covered employee or prospective employee has been convicted of any of the following disqualifying crimes:

(i) *Permanent disqualifying criminal offenses.* An applicant 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, if the applicant was either convicted of those offenses in a civilian or military jurisdiction, or admits having committed acts which constitute the essential elements of any of those criminal offenses within the seven years preceding the date of application; or the applicant was released from incarceration for the crime within the five years preceding the date of application.

(iii) *Under want or warrant.* An applicant who is wanted or under indictment in any civilian or military jurisdiction for a felony referenced in this section is disqualified until the want or warrant is released.

(iv) *Determination of arrest status.* When a fingerprint-based check discloses an arrest for a disqualifying crime referenced in this section without indicating a disposition, the State must determine the disposition of the arrest.

(v) *Waiver.* The State may establish procedures to allow for a waiver of the requirements of (b)(1)(ii) of this section under circumstances determined by the State.

(2) *Financial history check.* The State must conduct a financial history check on all covered employees and prospective employees identified under paragraph (a) of this section in a manner consistent with the Fair Credit Reporting Act. An employee's financial history shall be considered for informational purposes by the States only and shall not be considered a Federal disqualifier.

(3) *Lawful status check.* The State shall subject each covered employee to a lawful status check through SAVE.

(4) *Disqualification.* If results of the State's CHRC reveal a permanent disqualifying crime under paragraph (b)(1)(i) or an interim disqualifying offense under paragraph (b)(1)(ii); or the results of the lawful status check are unsatisfactory; the covered employee or prospective employee may not be employed in a position described in paragraph (a) of this section.

(c) *Appeal.* An individual who has been informed by the State that he or she may not be employed in a covered position as identified in paragraph (a) of this section as a result of the background check must be so informed and provided the opportunity to appeal. If a State determines that the individual does not meet the standards for the CHRC, is not trustworthy based on the financial history check, or does not have lawful status in the United States based on the lawful status check, the State must so inform the employee of the determination to allow the individual an opportunity to appeal to the State. Appeals based on the lawful status check should be appealed to DHS.

Subpart E—Procedures for Determining State Compliance

§ 37.51 Compliance—general requirements.

(a) To be in compliance with the REAL ID Act of 2005, 49 U.S.C. 30301 note, States must be meeting each and every standard of subparts A through D of this part, or have a REAL ID program that DHS has determined to be comparable to the standards of subparts A through D. DHS will find that a State is in compliance with REAL ID only if the State's certification submitted pursuant §§ 37.55 and 37.57 of this part establishes that all REAL ID driver's licenses and identification cards issued by the State on or after May 11, 2008 will meet the standards required under the REAL ID Act and this part.

(b) States must meet the requirements of subparts A through D of this part no later than May 11, 2008. In order to satisfy this requirement, a State must demonstrate compliance with this part

by submitting a certification and the documents specified in § 37.41 no later than February 10, 2008.

(c) States must demonstrate continued compliance by submitting a certification and documents specified at § 37.57 of this part as required by DHS.

§ 37.55 Initial State certification.

States seeking DHS's determination that its program for issuing REAL ID driver's licenses and identification cards is meeting the requirements of this part, must provide DHS with the following documents and information no later than February 10, 2008:

(a) A detailed narrative description of the State's program for issuing REAL ID driver's licenses and identification cards, including a description of the State's exceptions processing under § 37.11(h), the State's waiver processes under § 37.45(b)(1)(v).

(b) The State's Comprehensive Security Plan under § 37.41.

(c) A letter from the Attorney General of the State confirming that the State has the legal authority to impose requirements necessary to meet the standards established by this part.

(d) A copy of all statutes, regulations, administrative procedures and practices, and other documents that demonstrate the State's implementation program for this part.

(e) A certification by the Governor of the State reading as follows:

I, Governor of the State (Commonwealth) of __, do hereby certify that the State (Commonwealth) has implemented a program for issuing driver's licenses and identification cards in compliance with the requirements of the REAL ID Act of 2005, as further defined in 6 CFR part 37, and intends to remain in compliance with these regulations through [the last date of the current year].

§ 37.57 Annual State certifications.

Prior to January 1 of each year, each State must review its compliance with this part and certify to the Department of Homeland Security as prescribed in paragraph (a) of this section.

(a) The certification must consist of a Statement signed by the Governor of the State, reading as follows:

I (name of certifying official), (position title), of the State (Commonwealth) of __, do hereby certify that the State (Commonwealth) has continuously been in compliance with all requirements of the REAL ID Act of 2005 as further defined in 6 CFR part 37, since [the first day of the current Federal fiscal year], and intends to remain in compliance through [the last date of the current year].

(b) States shall provide DHS any changes to the information requiring certification, at least 30-days prior to the changes going into effect in the State.

(c) States shall supply the comprehensive security plan under § 37.41 of this part and a quarterly accounting of the State's use of its exceptions process, and the report required by § 37.15(f)(1) to DHS as part of the annual certification.

§ 37.59 DHS reviews of State compliance.

States' REAL ID programs will be subject to DHS review to determine whether or not the State meets the requirements for compliance with this part.

(a) *General inspection authority.* States must cooperate with DHS's review of the State's compliance during initial reviews, annual reviews, and at any other time. The State must provide any information requested by DHS, must permit DHS to conduct inspections of any and all sites associated with the application and verification process, manufacture, and production of driver's licenses or identification cards, and must allow DHS to conduct interviews of the State's employees or contractors who are involved in the application and verification process, manufacture and production of driver's licenses or identification cards.

(b) *Preliminary DHS determination.* After DHS reviews a State's certification and related documents, DHS will make a preliminary determination on whether the State has satisfied the requirements of this part. If, after review, DHS makes a preliminary determination, either that the State has not submitted a complete certification, or that the State does not meet one or more of the minimum standards for compliance under this part, DHS will inform the State of this preliminary determination.

(c) *State reply.* The State will have up to 30 calendar days to respond to the preliminary determination. The State's reply must explain what corrective action it either has implemented, or intends to implement, to correct the deficiencies cited in the preliminary determination or, alternatively, detail why the DHS preliminary determination is incorrect.

(1) The State must provide documentation of corrective action. Corrective action must be adequate to correct the deficiencies noted in the program review and be implemented on a schedule mutually agreed upon by DHS and the State.

(2) Upon request by the State, an informal conference will be provided during this time.

(d) *Final DHS determination.* If, after reviewing a timely response by the State to the preliminary determination, DHS makes a final determination that the State is not in compliance with this part, DHS will notify the State of the final determination. In making its final determination, DHS will take into consideration the corrective action either implemented, or planned to be implemented, in accordance with the mutually agreed upon schedule.

(e) *State's right to judicial review.* Any State aggrieved by an adverse decision under this section may seek judicial review under 5 U.S.C. chapter 7.

§ 37.61 Results of compliance determination.

(a) DHS will determine that a State is not in compliance with this part when it—

(1) Fails to submit the certification as prescribed in this subpart; or

(2) Does not meet one or more of the standards of this part, as established in a final determination by DHS under this section.

(b) A State shall be deemed in compliance with this part when DHS issues a determination that the State meets the requirements of this part.

§ 37.63 Extension of deadline.

A State may request a deadline extension based on the lack of a final REAL ID regulation to guide its implementation by filing a request with the Secretary no later than October 1, 2007.

(a) The request for consideration shall state that the State needs sufficient time to consider the final rule and will not otherwise be in a position to comply with the final rule.

(b) The Secretary has determined that, in the absence of extraordinary circumstances, such an extension request will be deemed justified for a period lasting until, but not beyond, December 31, 2009, providing that the requesting State complies with the requirements of this section.

(c) Any State receiving an extension for expedited consideration shall submit to the Secretary no later than six months from the date on which the extension is granted a Compliance Plan detailing milestones, schedules, and budgets allowing it to meet the requirements of the final regulation.

(d) After the Compliance Plan is submitted, the Secretary may require such progress reports or other information as the Secretary determines to be necessary to evaluate the State's progress toward compliance by December 31, 2009.

§ 37.65 Effect of failure to comply with this part.

(a) After May 11, 2013, any driver's license or identification card issued by

any State that DHS determines was not in compliance with this part when the driver's license or identification card was issued, is not acceptable as identification by Federal agencies for official purposes.

(b) If a driver's license or identification card issued when a State was in compliance with these regulations is renewed, the renewed driver's license or identification card is acceptable by Federal agencies for official purposes, only if the State is in compliance with these regulations at the time of renewal.

Subpart F—Non-REAL ID Driver's Licenses and Identification Cards

§ 37.67 Non-REAL ID driver's licenses and identification cards.

States that issue driver's licenses and identification cards that do not satisfy the standards of this part after May 11, 2008, must ensure that such driver's licenses and identification cards—

(a) Clearly state, on their face in bold lettering, as well as in the machine readable zone if the card contains one, that they may not be accepted by any Federal agency for Federal identification or other official purpose; and

(b) Have a unique design or color indicator that clearly distinguishes them from driver's licenses and identification cards that meet the standards of this part.

Michael Chertoff,

Secretary.

[FR Doc. 07–1009 Filed 3–8–07; 8:45 am]

BILLING CODE 4410–10–P