full legal name and apply it to all Federal records, rather than depending on the State DMVs to resolve this in the face of multiple Federal approaches. Due to discrepancies among naming conventions, one commenter suggested that DHS provide a list of most acceptable to least acceptable documents used to establish full legal name. Several commenters wrote that documents evidencing a name change may come from local or foreign government sources in addition to Federal and State governments.

Response: DHS agrees that there is no standard naming convention currently used by Federal agencies. It would be beyond the scope of DHS's rulemaking authority to impose such a convention on all Federal agencies. Nevertheless, the lack of a common Federal standard does not mean that DHS should not establish minimum standards for the States to follow as required by the REAL ID Act. However, based on comments received, DHS is slightly modifying the definition of the definition of "full legal name" to bring it closer to existing name conventions used by the Social Security Administration, the Department of State, and other issuers of source documents.

Comment: AAMVA and numerous States commented that the States need flexibility and DHS should drop the prohibition against using initials and nicknames. One State wrote that the name on the driver's license should be the one the person chooses to use, with the full legal name stored in the database and in the MRZ, and that without common naming conventions, it is imprudent to assume that a regulatory requirement forcing the public to adopt a single name will achieve any desired end. One State commented that it should be able to use an alternative name if the applicant's source documents clearly show a link between that name and the name presented on other source documents.

Response: As noted above, DHS agrees that where State law permits an individual to establish a name other than that contained on the identity document presented for a REAL ID driver's license or identification card, the State must maintain a record of how the name was established in a manner to be prescribed by the State. The use of initials or nicknames shall not be permitted, except to the extent that an initial is necessary to truncate a name longer than 39 characters in length, in which case the name should be truncated pursuant to ICAO-9303 standards. Where the individual has only one name, that name should be entered in the last name or family name field, and the first and middle name fields should be left blank. Place holders such as NFN and NMN should not be used.

Comment: Both States and victim advocacy groups objected to the full legal name requirement because the rule would not provide exceptions for victims of domestic violence. The rule would require that past names be included in DMV records, which would expose victims to danger. In addition, the SSA requires victims to change their names before changing SSNs and prohibits them from revealing previous names and SSNs. Commenters wrote that the proposed rule conflicts with this prohibition by requiring that the previous names be revealed as well as with the court orders under which many victims are granted new identities.

Response: The REAL ID Act does not include any exceptions for victims of domestic violence not to provide their full legal names. DMVs may want to take appropriate measures to protect the confidentiality of those records so that a stalker or victimizer could not use the DMV database to locate the individual.

Comment: Many commenters noted concern with the name requirement for the MRZ, particularly inclusion of the name history on the MRZ. States questioned whether some name histories would fit on the MRZ. Others questioned the need for the requirement if the history is available in the State DMV database and cited the potential for abuse. Many also commented that the requirement would result in a complete rewrite of States' systems and is one of the most costly parts of the rule. For example, one State commented that the 125-character field would delay its implementation for 3 to 5 years until it can obtain a new mainframe.

Response: DHS agrees with the comments and is no longer requiring that the name history be stored on the MRZ.

Comment: One State asked for guidelines for translating names from other alphabets: a name in the Cyrillic alphabet can be changed to the Latin alphabet a variety of ways. Another commenter recommended referencing the AAMVA name specifications generically rather than a particular edition. The commenter also suggested changing "Roman alphabet" to "Latin alphabet." Commenters noted other problems with the full legal name requirement, such as naming conventions in other countries and cultures, conversion of these names onto various immigration documents, and the "Americanization" of foreign names when living in the United States.

Response: DHS has changed "Roman" alphabet to "Latin" alphabet in the final rule. DHS is not requiring any particular transliteration method, but notes that both AAMVA and ICAO have published standards that address the issues raised in these comments.

2. Gender

Comment: Two States raised issues about how gender is determined for transgender individuals and whether gender will be included as a verifiable identifier through EVVE.

Response: DHS will leave the determination of gender up to the States since different States have different requirements concerning when, and under what circumstances, a transgendered individual should be identified as another gender. Data fields in EVVE are outside the scope of this rulemaking.

3. Digital photograph

Comment: A number of States objected to the requirement to take the applicant's photograph at the beginning of the licensing process because doing so would require extensive changes to State processes, facilities, and vendor contracts. According to one commenter, only seven States currently take an applicant's photo at the beginning of the process. One State requested a cost-benefit analysis for taking the photograph at the start of the process. One commenter suggested using an inexpensive image capture at first, then replacing the image with the final digital photo on issuance.

Response: Under § 202 (d)(3) of the REAL ID Act, States must subject each person applying for a driver's license or identification card to a mandatory facial image capture. Submission of an application for a driver's license occurs at the beginning of the licensing process, and as such, requires that the photo be taken at the beginning of the process. Additionally, from a law enforcement and operational perspective, an up-front image capture process serves as a deterrent to individuals attempting to present fraudulent documents or to "office shop" within a jurisdiction when their application may have been already denied in another office.

Comment: A number of commenters objected to the requirement for a color photograph because it would bar the use of laser engraving. One commenter stated that, photographs are better for checking identities. However, AAMVA and other States recommended that the required image be in color.

Response: DHS agrees with those commenters that a black and white photograph should also be acceptable in order to facilitate the use of laser engraving technology by States choosing to employ this technology to deter counterfeiters, and the altering and tampering of their drivers' licenses and identification cards. The final rule has been changed accordingly.

Comment: One commenter suggested that DHS replace the ICAO 9303 standard's aspect ratio with the AAMVA's aspect ratio, which is the Universal Camera Aspect Ratio.

Response: DHS believes the proposed ICAO aspect ratio, with an Image Width: Image Height aspect ratio range of 1:1.25 and 1:1.34, will accommodate the AAMVA Universal Camera Aspect Ratio of 1:1.33.

Comment: Several commenters wrote that requiring photographs could burden the free exercise of religion for some groups, such as Amish Christians and Muslim women. One commenter noted that banning the wearing of veils and scarves would require new State legislation. Another commenter asked DHS to clarify that a person may not wear any garment that affects the reliability of facial recognition technologies. Another State said the regulation should require States to refuse a license or ID to anyone who appears in disguise or distorts the face when photographed.

Response: As DHS stated in the preamble to the NPRM, the REAL ID Act requires a facial photograph, which serves important security purposes. Given these security 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-compliant driver's license or identification card. Many States now issue non-photo drivers' licenses or identification cards based on the applicant's religious beliefs. States may continue to issue these drivers' licenses or identification cards to such individuals and DHS recommends that these drivers' licenses and identification cards be issued in accordance with the rules for non-compliant drivers' licenses and identification cards at § 37.71.

While the final rule does not specifically address individuals who appear in disguise or who distort their face when photographed, DHS expects that States will implement their own procedures to ensure that the photographs are accurate representations of the individuals.

Comment: Some States objected to the requirement for a profile photograph for people under 21 years of age because it will defeat biometric facial recognition systems. One commenter suggested printing the cards with a different orientation to differentiate under-21 licensees while allowing for facial recognition technologies.

Response: A typographical error in the NPRM left the misimpression that DHS was requiring a profile photograph for individuals under age 21. The final rule does not require a profile photograph for people under 21, and instead requires a full facial digital photograph.

Comment: One commenter recommended that States be required to share their images. Another State commented that the requirement to retain images of people suspected of fraud would mean that they had to keep all images because the suspicion of fraud may occur long after the license is issued, and data storage costs would be significant.

Response: DHS agrees that there would be substantial value in preventing the acquisition of multiple identity documents if States were able to exchange images of their license holders with one another. DHS believes that the States have the same interest and therefore States must ensure that the same individual does not have multiple drivers' licenses or identification cards from the same State. DHS also encourages States to participate in AAMVA Fraud Early Warning System (FEWS) or similar system for exchanging information on fraud or attempted fraud in the issuance of drivers' licenses or identification cards. DHS believes that the volume of images of individuals who start, but do not complete the application process, will not be so great as to impose substantial data storage costs on the States.

4. Address of principal residence

Comment: One State noted that it has a "homeless exception" to its proof of residency requirement where proof of residency documents are waived if the applicant provides a letter, on letterhead, signed by the director of a homeless shelter, certifying that the individual is homeless and stays at that shelter. It suggested that this be an acceptable action under an "exceptions process" for the homeless. Other States voiced concern that the rule does not address the "truly homeless," those not living in a shelter.

Response: DHS agrees that a letter, on letterhead, signed by the director of the homeless shelter, certifying that an individual is homeless and stays at that shelter, should be sufficient to establish an individual's address of principal residence under a State's exceptions process. As noted above, States have wide latitude to address issues concerning an individual's address of principal residence within their State-specific exceptions process.

Comment: AAMVA, other commenters, and many States commented that DHS allow States the authority to provide for the confidentiality of individual's address of principal residence, including the categories of individuals who would be subject to the address exception. One commenter suggested that DHS devise standard rules governing address confidentiality rather than allowing each State to devise separate and unique requirements. One State claimed that a confidential address program is unnecessary.

Response: DHS agrees that States should have broad authority to protect the confidentiality of the address of principal residence for certain classes of individuals. DHS has added additional clarifying language in the final rule that should help to alleviate any uncertainties.

Comment: Numerous commenters claimed that the confidential address provision in the rule did not address all individuals who may have legitimate reasons for protecting their addresses from public disclosure. Commenters noted that § 37.17(f)(1) was too narrow and would not qualify individuals who would otherwise be protected under State law. Several States recommended additional address exceptions for the following categories: sitting and former judges, Federal officials in limited circumstances, covert law enforcement officers as long as the officer provides a letter of

authorization, State administrative personnel engaged in law enforcement, participants in the witness protection program, and victims of domestic violence. One commenter stated that the exemption should include family members when laws or court orders suppress the addresses of those individuals.

One commenter claimed that the partial exemption to the principal address requirement is inadequate by removing the option of not listing an address and relying solely on State laws that cover a limited number of individuals. The commenter noted that only 24 States have confidentiality programs in place, which is a requirement for the exemption to apply. Victims in the remaining jurisdictions will not be protected unless they can obtain a court order suppressing their addresses. Another commenter wrote that States have created formal address confidentiality programs and have also provided general measures of residential address privacy and this rule overrides these substantial protections.

Response: As noted above, DHS agrees that States should have broad authority to protect the confidentiality of addresses. DHS has clarified language in the final rule so that it is clear that a DMV may apply an alternate address on a driver's license or identification card if the individual's address is entitled to be suppressed under State or Federal law or suppressed by a court order including an administrative order issued by a State or Federal court.

Comment: A few States claimed that use of alternative addresses is justified on the REAL ID cards, but that the principal residence must be captured and stored in a secure database. They requested clarification from DHS on how States would meet the requirements related to the protection of the principal residence addresses. Another State

noted that it has no confidential address program, but it permits a post office box to be displayed on the identification document if requested, but again it retains the permanent address in a database. One commenter stated that the better level of protection would be to note in the MRZ that the individual's address is protected and provide a pointer to whatever relevant authority handles those addresses for that jurisdiction. This process would also serve a secondary purpose in that anyone seeking the address would make a request that could be logged and validated.

Response: DHS agrees that an individual's true address must be captured and stored in a secure manner in the DMV database even if an alternate address appears on the face and MRZ portions of the driver's license or identification card.

Comment: One commenter recommended that the final rule allow courts to issue administrative orders suppressing the collection of REAL ID information or its display on identification documents in any jurisdiction where the legislature has not acted to protect privacy.

Response: DHS agrees with this comment and has changed the final rule to reflect that an address may be suppressed by a court order including an administrative order issued by a State or Federal court.

5. Signature

Comment: Two States and another commenter stated that the rule needs to allow for people who cannot sign the card, such as minors, and older or disabled persons. If States use a signature match, an alternative process must be available.

Response: DHS agrees with these comments. Section 37.17(g) now provides that a State "shall establish alternative procedures for individuals unable to sign their

names." This language gives the States wide latitude in how to address situations where an individual is unable to sign his or her driver's license or identification card.

6. Physical Security Features

Comment: Numerous States and other commenters stated that DHS should provide security objectives or performance standards, and not specify particular technologies, materials, or methods. AAMVA wrote that States are using the AAMVA Driver Licensing/Identification Card Design Specification as the minimum standard and to change direction now would be costly for States. AAMVA further commented that restricting all State-issued drivers' licenses and identification cards to a single security configuration could introduce new security vulnerabilities rather than protect the drivers' licenses and identification cards against fraud. AAMVA wrote that it is not aware of any jurisdiction that uses all the listed security features with the proposed card stock in its card design or production. Numerous commenters stated that the proposed requirements would eliminate over-the-counter issuance systems and place an unnecessary financial burden on States.

Response: DHS understands that there are challenges States may face in producing secure drivers' licenses and identification cards. The final rule removes requirements to use specific technologies, and provides the flexibility for States to implement solutions using a combined set of security features that provide maximum resistance to counterfeiting, alteration, substitution, and the creation of fraudulent documents from legitimate documents. DHS will work with stakeholders to develop performance standards and a methodology for adversarial testing.

Comment: Commenters were concerned that DHS was not targeting its security

enhancement properly, and that increased security features would not accomplish the goal of reducing fraud. AAMVA and another State commented that major DMV fraud and abuse issues are not associated with the cards, but with source documents that cannot be verified, system breakdowns, and people who breach integrity. Another State commented that unless airports, Federal facilities, and nuclear plants have document authentication systems, implementation of REAL ID is without purpose. One State also stated that unless inspectors are trained in fraud detection or equipment is available for detection, fraud will continue. One commenter recommended that the AAMVA fraudulent document recognition training be used.

Response: DHS agrees, generally, that no single solution eliminates all fraud relating to an identity document. That is why the NPRM proposed, and the final rule requires, steps to improve internal procedures at DMVs as well as the physical driver's license or identification card issued by the States. DHS agrees that fraud detection training is an important element in an anti-fraud regime and endorses the use of AAMVA's fraudulent document recognition training or equivalent by the States.

Comment: AAMVA stated that States cannot consider making any changes until existing contracts with card integrators expire or they will face high penalties for breaking existing contracts; any change would require States to proceed though the competitive bidding processes, evaluate proposals, award new contracts, and implement the complex and expensive process of re-engineering their issuance processes. Any wholesale change in card design will be costly, complex, and time consuming. Several States also noted that contractual processes will slow implementation.

Response: DHS understands that existing vendor contracts make it difficult for some States to make changes during the term of their card contracts. The final rule provides flexibility in card solutions. DHS will require States to take appropriate measures to issue drivers' licenses and identification cards that are resistant to tampering, alteration or counterfeiting.

Comment: Commenters, particularly States that issue drivers' licenses and identification cards "over the counter," objected to check digit specification, unique serial number, application of variable data, and laser printing. One commenter supported associating card stock serial number with a customer. One State agreed with incorporation into the card of taggant (a radio frequency identification chip) and marker, but said that only State employees need to know if the State is using such embedded technology. One State noted that it uses seventeen overt, covert, and forensic security features to make counterfeiting difficult; it recommended that States use different designs and combinations of security features to deter counterfeiters. One commenter wrote that the proposed rule includes a requirement for an optically variable feature and suggests that a "diffractive optically variable feature" be included to enhance protection. The commenter said it is unclear how this feature enhances protection over existing State-issued drivers' licenses and identification cards as many already use such technology. The commenter recommended optically variable ink as a security feature. This ink technology, currently used in U.S. passports and outlined in the FIPS 201 security standards, is not reproducible using commonly used or available technologies, and requires much less training to authenticate quickly. No readers or special equipment are required to observe the color shifting effect, meeting the requirements in the proposed

rule for a Level 1 security feature. Additional forensic security, such as micro-flakes with etched on numbers, logos or words that are visible under low-power magnification can be included in the micro-flakes of the overt optically variable color shift technology, meeting the requirements in the proposed rule for a Level 2 and Level 3 security features.

Response: The final rule provides for a performance-based, not prescriptive, approach to card solutions. Specific security requirements are not mandated in the rule. However, the final rule includes requirements for three levels of document security designed to provide maximum resistance to counterfeiting, alteration, substitution, and the creation of fraudulent documents from legitimate documents that are not reproducible using common or available technologies. DHS encourages States to explore the range of existing and still-to-be developed technologies in this area. The final rule requires States to use card stock and printing materials that are not widely available commercially in order to significantly decrease the likelihood that a driver's license or identification card could be easily counterfeited or altered.

Comment: One commenter recommended inclusion of a digital signature as a Level 3 security feature.

Response: The final rule provides for performance-based, not prescriptive requirements for implementation. While digital signatures offer a higher level of security, States may choose to invest in other, similarly secure technologies. DHS encourages States to consider the use of this and other security features.

Comment: States asked for clarification as to the meanings of "inspector," "microline text," "micro print," "external surfaces," "taggant," and "marker."

Response: DHS has removed the requirements involving these terms, so does not need to clarify these terms.

Comment: Two commenters stated that security features should not make it impossible to copy or create a digital image of a license, and that the rule should make it clear that any print on the image must not obscure the features. One State asked that DHS remove language forbidding reproducible security features and retain § 37.15(f)(2).

Response: DHS agrees that the security features employed should not make it impossible to copy or create a digital image of a license. Many private sector industries, including the banking sector, often need to reproduce and retain a copy of an individual account holder's driver's license or identification card. DHS also agrees that print on the image should not obscure the individual's features.

Comment: One commenter recommended incorporating some security features in the substrate.

Response: The final rule requires level 1, 2 and 3 security features that provide multiple layers of security, and States may adopt security features that meet their needs, including incorporating security features into the substrate.

Comment: One commenter stated that requiring a color photo and laser printing means that two printers will be needed.

Response: The final rule allows for either a color or black and white photograph. Laser engraving, while a very effective security measure, is not a requirement of this rule.

Comment: One State commented that it currently uses adversarial testing for its cards and provided detailed information on its process. AAMVA and several States said that there are no adversarial testing standards and that DHS should develop them and

either take responsibility for testing the cards or certify the testing organizations. Another commenter recommended that there should be a single center for adversarial testing using a single set of criteria to avoid the undue influence of vendors and disparate standards. Some States suggested alternatives to adversarial testing, such as card design security programs or security audits. One commenter suggested that adversarial testing occur only if the State card has changed rather than annually. Another commenter recommended testing every five years or at contract changes.

Response: The development of standards and adversarial analysis and testing of drivers' licenses and identification cards is an effective approach to ensuring that these documents provide maximum resistance to counterfeiting, simulation, alteration and creation of fraudulent drivers' licenses and identification cards. DHS will work to develop performance standards and adversarial analysis and testing.

Independent adversarial testing is an important tool in limiting the ability of someone to tamper, alter, or counterfeit a driver's license or identification card. DHS agrees with the comments that there are no recognized testing standards to date and a lack of available and accredited testing facilities. Therefore, DHS has removed the requirement for States to obtain an independent adversarial test of their card security.

Comment: Numerous commenters objected to the card stock requirement, stating that the NPRM design specification essentially calls for polycarbonate material and AAMVA and its members do not support polycarbonate as the only option for the cards. This material is not used anywhere in the United States today, is the highest cost card material in production today, and is only available from a limited number of vendors, which negates State requirements for competitive bidding. Another commenter

noted an inconsistency between polycarbonate card stock and the requirement to meet ICAO 9303. The ICAO standard requires a color photo, but polycarbonate card stock allows only black and white photos.

Privacy groups supported use of polycarbonate cardstock in conjunction with laser engraving because laser engraving on other card stocks may be removable. One commenter indicated that other stocks would function as well. Another commenter stated that requirements for card stock durability should be based on the renewal period used by the State. One State asked to whom missing card stock should be reported.

Response: The final rule reflects a less-prescriptive approach to card security, and does not mandate the use of a specific card stock and prescriptive security features. The final rule requires States to use card stock and printing methods that are not widely available commercially in order to significantly decrease the likelihood that a driver's license or identification card can easily be counterfeited or altered. States should develop and utilize a system of reporting missing card stock and other secure supplies and equipment related to the production of drivers' licenses and identification cards to other State DMVs and law enforcement.

7. Machine Readable Technology

Comment: Privacy groups and several States recommended laws limiting the collection and storage of Machine Readable Zone (MRZ) data by third parties. Several other States commented on the importance of accessibility for law enforcement and noted that the same information is available on the front of the identification cards in human-readable form. Some commenters wanted MRZ access restricted to law enforcement, while others supported also providing access for bars and liquor stores to help prevent

underage drinking but limiting their collection and storage of the personal information. One commenter stated that nothing in the REAL ID Act authorizes Federal agencies to read and collect information contained in the MRZ and cited to the Conference Report statement that the MRZ must only be able to be read by law enforcement officials. One commenter opposed any indication in the MRZ that a person was an owner or buyer of firearms or was licensed to carry a firearm; the commenter also asked that DHS forbid the inclusion of this information unless required by State law.

Response: The REAL ID Act does not provide DHS with authority to prohibit third party private-sector uses of the information stored on the REAL ID card. As noted in the proposed rule and the PIA issued in conjunction with the rulemaking, at least four States (California, Nebraska, New Hampshire, and Texas) currently limit third-party use of the MRZ, and AAMVA has issued a model Act limiting such use. DHS encourages other States to take similar steps to protect the information stored in the MRZ from unauthorized access and collection. In response to commenters urging that the rule limit Federal agency access to the MRZ, DHS is not aware of any current plans by Federal agencies to collect and maintain any of the information stored in the MRZ. If a Federal agency should decide to use the MRZ to collect and maintain personally identifiable information in the future, any such information collected from the MRZ will, of course, be subject to the protections of the Privacy Act and other Federal laws and policies regulating the use and handling of personally identifiable information. This final rule does not require (and the NPRM did not propose) that the MRZ contain any information about firearm ownership.

Comment: Many commenters suggested data elements that should or should not be in the MRZ. AAMVA stated that the final rule should limit the MRZ elements to those set out in its driver license card design standard. Another commenter wrote that DHS should set the minimum data elements in the MRZ at zero and the maximum at full legal name, date of birth, and license number. Other commenters stated that data on the MRZ should be limited to what is on the face of the document. One State recommended inclusion of the issuing State in the MRZ to facilitate the routing of NCIC inquiries by law enforcement agencies using in-car bar code reading equipment. Another commenter suggested limiting the MRZ data to a pointer that does not correspond to the ID number that would link to a database limited to law enforcement. One commenter recommended including the digital image in the MRZ using the ISO/IEC 18013-2 standard. Two States opposed including an inventory control number (ICN). One commenter objected to the PDF standard because the NPRM preamble had referenced adopting most of the data elements in the 2005 AAMVA Driver's License/Identification Card Design, which includes coding for race.

Response: The final rule mandates that the States use the PDF417 2D bar code standard with the following defined minimum data elements: expiration date; holder's legal name; issue or transaction date; date of birth; gender; address; unique identification number; revision date (indicating the most recent change or modification to the visible format of the license or identification card); inventory control number of the physical document; and State or territory of issuance. The proposal in the NPRM to include the full name history, including all name changes, has been dropped. Race is not a data

element contemplated in this rulemaking and the reference in the NPRM to the AAMVA standard was not intended to include race as a data element in the MRZ for REAL ID.

The majority of commenters on the issue of data elements recommended limiting the data elements to those needed by law enforcement and the DMVs to carry out their duties. The final rule sets the minimum elements to include, but recognizes the authority of the individual States to add other elements such as biometrics, which some currently include in their cards.

Changes in technology in the future may enable the States to reduce the elements to a pointer that would electronically link to a database and provide only authorized parties access to information that today is stored in the MRZ. The current technology available to State DMVs and most law enforcement officers, however, does not provide that capability.

Comment: Several commenters said the 2D barcode is easily copied and reproduced. One commenter supported the 2D barcode, but noted that it is not meant to be a security feature; the 2D barcode does not allow an upgrade of an encryption scheme, does not employ dynamic forms of authentication, does not store audit trails, and does not use other security features. One commenter stated that the rule for the barcode was insufficient, particularly that there was no barcode standard specified which would facilitate the common machine readable technology requirement mandated by the REAL ID Act. Two existing standards could provide the basis for what is needed: one is the AAMVA format and the other is the format in the draft of part 2 ISO standard 18012. However, the proposed rule required fields that are specified differently or are just not in either of these standards. One commenter objected to the standard because the selected

version includes coding for race. One commenter stated that mandatory requirements make it difficult to keep up with technology. A security group and one State stated the bar code should include a revision date.

Response: DHS recognizes that a 2D barcode may have security vulnerabilities and technology limitations compared to other available technologies. However, the PDF417 2D barcode is already used by 45 jurisdictions and law enforcement officials across the country. A different technology choice could hamper law enforcement efforts and may pose an additional financial burden on the States. DHS supports efforts of States to explore additional possible technologies in addition to the PDF417 2D barcode.

DHS disagrees with the notion that the standard selected should be rejected because it includes coding for race. DHS has never stated that race should be encoded on the license, and specifically stated in the proposed rule that it was not incorporating wholesale the card data elements currently required by AAMVA.

Comment: One commenter supported the decision to omit an RFID device. It stated, however, that the NPRM does not discuss what information from a card should be made available digitally and what purpose it would serve.

Response: DHS is not requiring that States employ RFID in REAL ID Act cards; rather the only technology required by the final rule is the use of the PDF417 bar code, which most States already use on their cards. The information stored on the MRZ enables law enforcement officers to compare the information on the MRZ with the information on the front of the card to determine whether any of the information on the front has been altered and to automatically populate law enforcement reports, increasing officer safety. The ability to run the MRZ through a scanner device also enables an

officer to quickly retrieve the information on the card and request from their dispatch office additional information on the individual, while maintaining visual contact with a suspect, a safety consideration for the officer.

8. Encryption of MRZ information

Comment: Commenters were divided on whether some or all data in the MRZ should be encrypted. In general, groups concerned with privacy issues supported encryption, although one commenter argued that encryption would provide a false sense of security. Three States supported encrypting MRZ data. Groups supporting encryption cited the following:

--The capture of data by other users, such as financial, retail, or commercial institutions that could retain, use, and sell the personal data.

--The possible inclusion of additional private information in MRZ, such as residential address, race, [trans]gender, or legal name history that could expose the holder to harm if captured and revealed.

--Congressional intent to limit use of the data to law enforcement.

Some commenters stated that if DHS does not mandate encryption, it should at least not prohibit it. Others supported encryption of only some data, specifically data not available on the front of the card. One supporter stated that DHS should have done a comprehensive analysis of encryption systems and their costs and presented that data.

Numerous other commenters, including the States and AAMVA, opposed encrypting the data. Other commenters were divided among those who believed it is feasible to encrypt the data, those who considered it infeasible, and those who offered

alternative technologies, particularly smart cards and public key infrastructure. Commenters opposing encryption cited the following reasons:

--The difficulty of managing encryption keys that could be used to decrypt any REAL ID. If a single key was used, once the key was compromised, every driver's license issued with the key would be insecure. If multiple keys are used (e.g., different keys for each State), then every law enforcement agency would have to be able to access all of the keys. Multiple keys would limit the threat because key compromise would affect fewer drivers' licenses, but would increase the difficulty of using the MRZ data across the country. Once a key is compromised, any license issued using that key would have to be replaced to be secure.

--The cost of systems for law enforcement. The costs cited included the cost to replace existing readers plus the cost of setting up an encryption system and the ongoing costs of managing keys.

--The additional time required for law enforcement. Particularly if multiple keys are used, law enforcement and DMV officials may need more time to read the data. This added time requirement would limit the ability to check the validity of documents quickly, particularly those from other States.

--The inability of non-law enforcement to use the data to verify the validity of the information on the face of the card. Businesses also use the MRZ data to determine if the document is genuine. Eliminating that ability would harm businesses that rely on the driver's license and would affect the ability of restaurants and bars to confirm ages. These businesses can help identify criminal use of false documents using the MRZ.

Some commenters argued that the government should set limits on the retention and use of the data rather than encrypt the MRZ.

--The futility of encrypting data present on the front of the card. Commenters stated that if the data included in the MRZ are readable on the front of the card, encrypting the MRZ provides no protection because optical scanning readers are capable of translating the card data into a database. The information can also be copied or transcribed.

Response: DHS considered the many comments on this issue and acknowledges that the skimming of the personally identifiable information from the MRZ raises important privacy concerns. Nevertheless, given law enforcement's need for easy access to the information and the complexities and costs of implementing an encryption infrastructure, no encryption of the MRZ will be required at this time. If the States collectively determine that it is feasible to introduce encryption in the future, DHS will consider such an effort, as long as the encryption program enables law enforcement to have easy access to the information in the MRZ. Moreover, DHS, in consultation with the States, DOT, and after providing for public comment, is open to considering technology alternatives to the PDF417 2D bar code in the future to provide greater privacy protections.

J. Validity Period and Renewals of REAL ID Drivers' Licenses and Identification Cards

1. Validity period

Comment: At least two commenters said that the proposed eight-year validity period is too long, because it would give counterfeiters and forgers too much time to

learn how to simulate or alter cards in circulation. The groups recommended that DHS require States to adopt a validity period of no more than five years. AAMVA and one State said that State DMVs should be allowed to determine the duration of their licenses based on business processes and needs. A few States said that a validity period of no more than eight years would create difficulties for elderly and some disabled persons who are clearly not national security risks. These States asked for the flexibility to grandfather these populations or to issue cards with extended validity periods.

Response: The REAL ID Act establishes a maximum license validity period of eight years. Nothing in the Act or the rules precludes a State from adopting a shorter validity period for business, security, or other needs.

2. Reverification of source document information

Comment: AAMVA and several States expressed strong opposition to the requirement that States re-verify information and source documents for renewals and replacements of drivers' licenses and identification cards. They said that this requirement would be costly, burdensome, and unnecessary in part because of the processes that many States already have in place for renewals and replacements. In addition, some commenters claimed that the requirement to re-verify source documents such as address documentation is impossible to comply with because there is no electronic system to do so. One State DMV pointed out that because Federal and State databases are not updated in real time, it is likely that changes would not be immediately verifiable.

One State supported requiring re-verification of birth certificates because changes to the birth certificate, such as a name change, could be made after the original birth certificate verification occurred. This suggestion would also allow for matching against

State death information to prevent fraud. Another State endorsed the re-verification of information for temporary REAL ID licenses and for driver and ID card holders who do not have Social Security numbers.

Response: DHS agrees with the comments that it is not necessary to re-verify all source documents at renewal. DHS proposed this requirement in the NPRM since it recognized that the quality of recordkeeping in both Federal and State databases would improve over time. Instead DHS has amended the rule to require reverification of SSN and lawful status prior to renewal and verification of information that the State was previously unable to verify electronically.

Comment: Several State DMVs asked DHS to clarify exactly what they would need to do to "re-verify" information. For example, one State asked if States would be required to verify each source document and imaged piece of information if electronic verification systems were not available at the time of initial enrollment. One State asked if States could use original source documents to re-verify applicant information if the documents have expired since the date of original verification. Another State asked DHS to explain the difference between "verified" and "validated" as referenced in § 37.23(b)(1)(ii) of the NPRM.

Response: As noted above, DHS is not requiring States to re-verify source documents at renewal. However, States must reverify the SSN and lawful status upon renewal and electronically verify information that the State was previously unable to verify electronically.

Comment: AAMVA said that DHS should allow States to determine if they want to re-verify information that has already been verified by another State. AAMVA

said that the new State of residency should be able to determine whether to "re-vet" an applicant's information. One State requested that DHS allow a license transferred from another State to be renewed or replaced remotely, even if the new State of residence does not have electronic copies of the applicant's identity documentation. One State said that the renewal of a REAL ID-compliant card should only require the minimum combination of a REAL ID document and some proof of address. Another State suggested that States be allowed to exempt from re-verification applicants who have been verified at initial enrollment as U. S. citizens and who have had no changes to name or Social Security information. A few commenters mentioned that a birth certificate should not be re-verified if there was a copy of it maintained at the DMV.

Response: The NPRM did not propose any requirements for how a State should treat a REAL ID issued by another State except to propose that a REAL ID driver's license or identification card be accepted as an identity document, to establish name and date of birth. When an individual moves from one State to another, the new State would still be required to verify the individual's SSN and ensure that he or she is lawfully present in the United States

3. Renewals

Comment: AAMVA recommended that § 37.23 be entirely stricken except for paragraph (b)(2)(iii) of the NPRM, which would require holders of temporary REAL ID cards to renew them in person each time and to present evidence of continued lawful status.

Response: DHS disagrees with the comment and believes that it is necessary to have standards governing the renewal of a REAL ID-compliant driver's license or identification card.

Comment: One commenter wrote that the rule would make it far more difficult and expensive for current holders of a commercial driver's license (CDL) to renew or replace their licenses, that delays and the expense in having a license renewed or reissued are particularly important for this segment of the population, and that they might force drivers to seek other employment altogether.

Response: DHS disagrees with this comment. DHS has not been presented with evidence that CDL holders will be affected disproportionately by the REAL ID requirements or that the REAL ID requirements will force commercial driver's license holders to seek other employment.

Comment: Commenters expressed strong opposition to the restriction that remote transactions would be allowed only if "no source information has changed since prior issuance" (§ 37.23(b)(1) of the NPRM). In particular, many States, AAMVA, and other commenters wrote that applicants should be able to make address changes without having to appear in a DMV office, and that only material changes (e.g., name change) should prompt the need for an in-person visit. In general, commenters wrote that they do not currently require an office visit for address changes, and some said they do not issue a new card when notified of an address change. They said that requiring in-person visits for address changes would dramatically increase the number of visitors to DMV offices, with huge cost increases for State agencies (which some DMVs said the Federal government should cover), without necessarily improving national security. Some States

further commented that making address changes more difficult for customers will result in these individuals simply not notifying the motor vehicle department of new addresses, which creates greater problems for State and local government and law enforcement.

Response: DHS agrees with these comments and has removed the requirement that an address change must be accomplished through an in-person visit to the DMV. Additionally, there is no requirement in the final rule for States to issue a new card when notified of an address change.

Comment: DHS received several comments on some of the methods listed in the preamble for authenticating identity prior to issuing a renewed license.

Response: Since DHS is only requiring that States establish a procedure to ensure that the proper individual is receiving a renewed document and is not requiring any specific method, these comments are not discussed as they are deemed outside the scope of the regulation.

Comment: AAMVA commented that the requirement that every other renewal take place in-person to allow for an updated photo would penalize residents of States with shorter renewal cycles. One State suggested that § 37.23(b)(2) of the NPRM should be changed to require in-person renewals and recapture of a digital image once every sixteen years, regardless of the period of validity of a State's cards. Two commenters stated that allowing sixteen years between photo updates might be too long because a person's appearance can change significantly during that time, and that the usefulness of the photos for facial recognition (manual or computerized) would greatly diminish over a sixteen-year time period. One State recommended that DHS adopt a ten-year in-person renewal cycle. Two States commented that exceptions to in-person renewals should be

established for active military and the elderly.

Response: DHS disagrees with the comments and is retaining the requirement that a new photo be taken at every other renewal of a REAL ID driver's license or identification card. Enabling States to maintain their own renewal cycles permits States to plan for the flow of people through the DMVs. While DHS agrees that an individual's appearance can change significantly over sixteen years, DHS has concluded that an every-other-cycle photo requirement will meet State needs to reduce in-person visits at the DMVs while not posing an unacceptable security risk. States are free to impose a more frequent photo requirement.

4. Reissuance of documents

Comment: One State said that it would be overly burdensome to require all applicants for replacement drivers' licenses or ID cards resulting from lost, stolen, or mutilated documents to personally appear at a DMV office. Another State wrote that, in many instances, the affected customer will not have the supporting documents readily available, which may result in some individuals driving without a license.

Response: DHS agrees with the comments. In the final rule, States may replace a lost, stolen, or mutilated document without requiring an in-person transaction. Current State practices will dictate what documentation needs to be presented for replacement drivers' licenses and identification cards.

Comment: Some States, AAMVA, and several other commenters recommended against requiring a new card for address changes and asked that DHS allow States to propose interim methods of tracking address changes between renewal cycles without the requirement for issuance of a replacement card (unless State law requires it).

Response: DHS agrees with the comments. The final rule does not mandate that a State reissue a driver's license or identification card for an address change unless otherwise required by State law.

Comment: A number of States suggested that the definition of "reissued" be changed to indicate that the license contains material changes to the personal information on the document. An applicant for a "reissued" document would be required to personally appear at a DMV office to provide proof of the change. Furthermore, the State suggested that DHS create a definition of "duplicate" as a card that was issued subsequent to the original document that bears the same information and expiration date as the original.

Response: DHS agrees with the comments. The final rule does not mandate a personal appearance at a DMV for a reissued driver's license or identification card unless material information, such as name or lawful status, has changed. The final rule adopts the proposed definition for a duplicate card.

K. Source Document Retention

Comment: AAMVA expressed concern about the proposed requirements dealing with transferring document images and linking document images to the driver record, and opined that the requirement to color scan and exchange documents using AAMVA's Digital Image Exchange program is misplaced. Another commenter stated that this program deals only with photos and that "it would be a giant leap to consider its use for documents." Several commenters objected to the costs of purchasing scanners, using computer storage space, retaining color images, and integrating the image into the driver record. Some commenters believed the document retention period should be the same for

paper copies and electronic storage, while others believed that the retention period for paper copies should be shorter than electronic. A few commenters pointed out that the Driver Privacy Protection Act and State laws had their own record retention requirements. Some commenters objected to the storage of documents containing sensitive personal information as such documents are attractive target for criminals and hackers, and thereby pose significant privacy and security risks.

Response: The specific record retention period for imaged documents and paper documents is required by the REAL ID Act and the final rule applies those time periods. However, DHS agrees with the comments that some source documents may contain sensitive personal information and has modified the document retention requirements for birth certificates. Under the final rule, a State shall record and retain the applicant's name, date of birth, certificate numbers, date filed, and issuing agency in lieu of an image or copy of the applicant's birth certificate, where such procedures are required by State law and if requested by the applicant.

L. Database Connectivity

Comment: AAMVA stated that DHS has yet to provide specific information on how this "query" system will work and does not expect to provide that information until the comment period is over. AAMVA wrote that final rulemaking should not take place until there is opportunity for another round of comments and an extension of compliance dates.

Privacy groups argued that the proposal does not define security standards or a governance structure for managing any of the shared databases and systems. In their view, this abdication places the States in an impossible position: they are being forced to

make their own citizens' personal information available to every other State with no guarantee of privacy or security.

One commenter recommended that the PCI Data Security Standards that apply to the credit card industry should be applied to DMV databases. One group suggested a decentralized query system that allows States to check all other States to see if an applicant already holds a REAL ID and returns a yes or no answer, rather than providing detailed data. One commenter recommended audit logs and audits to ensure compliance with privacy policies.

Response: DHS has provided a brief overview of the proposed architecture for data verification and State-to-State data exchange in the sections above. This architecture will likely build on the existing architecture of AAMVAnet and the systems design principles of its hosted applications. The proposed architecture will also build upon the security, privacy and governance principles that have guided AAMVA and the States for decades.

In addition, DHS will work with DOT, AAMVA and the States to reinforce the security and privacy features of this communications and systems architecture.

Comment: A commenter stated that DHS had exceeded its authority in the requirement that interstate access must be "in a manner approved by DHS." This commenter stated that since the rule does not describe, even in general terms, what the approval is based upon, States are left to guess at the DHS criteria for approval. Since the database exchange and the connectivity thereto are of utmost importance to States, the conditions upon which approval will be based need to be specified in the rule. They

should not be provided by some yet to be developed guideline issued by DHS after the rule has become final.

Response: DHS will work with DOT, AAMVA, and the States to develop a path forward for both verification systems and State-to-State data exchange, including criteria DHS will employ to evaluate the adequacy, security, and reliability of such data exchanges.

M. Security of DMV Facilities Where Drivers' Licenses and Identification Cards are Manufactured and Produced

1. Physical security of DMV facilities

Comment: A few States said the security requirements would force closure of many DMV offices. At least one State said that the security requirements would lead to closure of remote offices, and that this could lead the State to opt out of complying with REAL ID requirements.

Response: In general, DHS does not agree with comments that indicate a State would prefer to have a security vulnerability rather than take the necessary steps to close it. There have been a number of well-documented instances where DMV offices have been burglarized and the equipment and supplies to manufacture drivers' licenses and identification cards taken, highlighting the need to ensure that adequate procedures are in place to protect the equipment and supplies necessary for the production of REAL ID drivers' licenses and identification cards. Protecting these materials and equipment are critical to reducing the possibility of fraud and identity theft.

Comment: While a few States supported the proposed ANSI/NASPO-SA-v3.OP-2005, Level II standard, numerous States said that this standard was intended to

apply to manufacturing facilities, not to the issuance of drivers' licenses. The commenters opposing use of the ANSI/NASPO standard stated that until a reasonable standard is developed, States should have the flexibility to determine what works for their issuance processes. Privacy groups are concerned that without a uniform standard, States could have 56 different security and privacy policies with different levels of protection.

One State supported a narrow application of the ANSI/NASPO standard only to the DMV facility containing the database on license holders, while another State thought that the standards should apply only to the DMV production facilities. One commenter wrote that the NASPO standard needs to be reviewed every two years and that requirements should be added throughout the supply chain.

Response: DHS agrees with the comments that the proposed NASPO standard may be more appropriate to manufacturing and production facilities, as opposed to issuance sites. DHS is not requiring the use of the ANSI/NASPO standard in the final rule, but commends to the States the proposed standards as a good practice for securing materials and printing supplies.

Comment: One commenter proposed additional requirements for alarm systems, disposals, and suppliers. Another commenter suggested allowing DMVs to secure part of a building, rather than the whole building. The commenter wrote that the standard did not address the security of work stations and recommended biometric passwords. One commenter noted that providing the license directly to the person, rather than mailing it, was more secure; one State noted that the Post Office does not guarantee delivery.

Response: The final rule specifies what must be addressed in a security plan, including physical security of the buildings used to produce drivers' licenses and

identification cards, storage areas for card stock and other materials used in card production, and security of Personally Identifiable Information (PII).

If a DMV is located in a building shared by other offices or tenants, the area dedicated to the manufacture or issuance of drivers' licenses and identification cards, storage of card stock and related materials, and PII must be secured in such a fashion to prevent unauthorized access. This requirement covers any equipment utilized to produce drivers' licenses and identification cards as well as storage, access and retrieval of PII. States will determine how these items are protected in their security plans.

The rule does not mandate central issuance versus over-the-counter issuance.

2. Security plan

Comment: One State said that DHS had exceeded its authority under the Act in the requirement that a State's security plan address "reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of ... personal information stored and maintained in DMV ... information systems." Another State wrote that the Act does not authorize DHS to compel States to establish or make available standards or procedures for safeguarding the information collected by motor vehicle agencies. AAMVA asserted that tools such as information security audits, individual employee access audits, employee confidentiality polices, and privacy and security plans are already used in many DMVs.

Privacy groups commented that the rule must provide meaningful privacy and security protections and that the lack of clear privacy and security guidance in the Act does not preclude DHS from providing strong protections in the regulations. In fact, they urged DHS to include specific standards or minimum criteria against which the State

plans could be evaluated.

At least two States objected to the provision that DHS could require "other information as determined by DHS." The States argued that any further requirements should be agreed upon and clearly identified in the regulations. One State said that unspecified requirements should not be left to DHS to develop outside of the regulatory process. Another State wrote that the access badge requirement is unrealistic.

Response: DHS believes that it has the authority to require States to take reasonable measures to safeguard the confidentiality of PII maintained in DMV information systems pursuant to the REAL ID Act. DHS believes that inherent in the Act's requirement that States must provide electronic access to the information contained in their databases is the principle that such information must be protected, and this concept is supported in the legislative history for section 202(d)(12) of the Act which states that "DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards ...." H.R. Rep. No.109-72, at 184 (2005)(Conf. Rep). Failure to protect the PII held in DMV databases could result in identity theft and undermine the very purpose of the Act, which is to strengthen the validity of the cards. DHS also believes that it can require States to provide other, reasonable information that DHS determines is necessary in the future without requiring future rulemaking.

Comment: AAMVA and several States requested guidance on what "written risk assessment of each facility" means and a template. Another State asked for guidance on which law enforcement officials should be notified. One State recommended that the rule

limit the amount of data in any State's database and create stronger protections for information to limit the danger of aggregating information on 240 million Americans.

Response: DHS, DOT, AAMVA and the States will work together to develop best practices for risk and vulnerability assessments as well as for security plans for DMV facilities.

Comment: A trade association objected to the lack of standards for the security plan and further stated that because the State databases must be interconnected, the lack of standards would mean that the weakest plan implemented by any State would put all States at risk. DHS should require clear, strong, and verifiable minimum security measures. An association said that DHS was ignoring the threat posed by insiders, employees and contractors. According to this association, the rule should recognize the threat and the importance of training to mitigate those risks.

Response: The final rule specifies what must be addressed in a security plan, including: physical security of the buildings used to produce drivers' licenses and identification cards, storage areas for card stock and other materials used in card production; security of personally identifiable information including reasonable administrative, technical, and physical safeguards, a privacy policy, and limits on disclosure; document and physical security features for the face of the driver's license or ID card, including a description of the State's use of biometrics and the technical standards utilized (if any); access control, including employee identification and credentialing, employee background checks, and controlled access systems; periodic training requirements in fraudulent document recognition for covered employees; emergency/incident response plan; internal audit controls; and affirmation that the State

possesses both the authority and the means to produce, revise, expunge and protect the confidentiality of REAL ID drivers' licenses and identification cards issued in support of Federal, State or local criminal justice agencies or similar programs that require the safeguard of a person's identity in the performance of their official duties. Such requirements shall also apply to contractors involved in the manufacture or issuance of REAL ID-compliant drivers' licenses and identification cards.

3. Background Checks for Covered Employees

Comment: Generally, States did not support the proposed background check provisions. A few States objected to these provisions as too broad and impractical. AAMVA stated that these requirements are a Federal intervention into State personnel rules and one commenter stated that these provisions are a particularly invasive intrusion on State autonomy to decide the qualifications and conditions of persons within its employ, which is a fundamental attribute of State sovereignty. States also objected to § 37.45(c), the provision instructing the States to notify persons of unfavorable checks and provide them appeal rights, and claimed that this provision may grant rights nonexistent in State law.

Numerous States said that background checks and the standards applied should be at the discretion of the State and not required. AAMVA and several States suggested that existing employees should be grandfathered in to allow States to determine whether they want to do complete background checks on such employees.

Response: DHS disagrees that it cannot require background checks of covered employees. Such checks are a necessary step to protect against insider fraud, one of many vulnerabilities to a secure licensing system. DHS also disagrees with the concept

of "grandfathering" existing personnel since there is no way to know in most States whether employees who have not been subject to a background check would satisfy this important requirement. Further, § 202(d)(8) expressly directs States to "[s]ubject all persons authorized to manufacture or produce drivers' licenses and identification cards to appropriate security clearance requirements." The background checks required under this final rule are authorized by and consistent with that statutory mandate. The statute does not provide for an exemption for personnel employed by a State DMV before the effective date of the Act or this final rule and thus DHS cannot include a grandfather clause in this rule.

Comment: Some States believed that DHS has exceeded the authority granted by the Act on background check provisions because of its expansive definition of "covered employees." These States asserted that DHS is without authority to extend the background check requirements beyond employees who "manufacture or produce" cards. Similarly, one State asked that employees at branch offices who are not involved in the production and manufacture of drivers' licenses or identification cards be exempt from the background check requirements. One State noted that the rule attempts to subject "covered employees," "prospective employees," and "applicants" to the criminal history record check, yet only defines the term "covered employee."

Response: DHS disagrees that its definition of a covered employee is too expansive. DHS, the agency charged with interpreting and enforcing the Act, interprets "persons authorized to manufacture or produce" REAL ID cards to include those individuals who collect and verify required source documents and information from applicants as such information is a necessary part of the production of a REAL ID card.

It would be illogical to cover only those DMV employees and contractors who carry out only the physical act of cutting or printing a license while exempting those individuals who interact with the public and may be most able to introduce fraudulent information into the system and thus thwart the intent of the Act.

Comment: Commenters wrote that States currently only undertake background investigations at the time of hiring, and that since existing employees are not applicants, it is entirely reasonable for labor organizations and permanent State employees not covered by collective bargaining agreements to argue that non-probationary employees fall outside the scope of the background check provisions. Some commenters claimed that the requirement that all designated employees, including those who are already employed, undergo background investigations is contrary to many State labor contracts and personnel practices. Numerous employees were hired under terms and conditions not requiring a security clearance. Should these employees be disqualified under the new regulations, States may be obligated to provide them with alternative employment or severance.

Response: As noted above, DHS believes that it would be a significant security vulnerability to exempt current DMV employees from a background check.

Comment: One commenter claimed that the use of the phrases "applicant" and "application" in the rule governing interim disqualifying criminal offenses poses a practical problem, since the time periods are defined in terms of the date of the application. Existing employees would have been considered applicants on the date they filed the application for the position in which they are currently employed, which may be well outside the time period that applies to interim disqualifying offenses (five years from

the date of application). Thus, commenters argued, the time period for interim disqualifications should start from the date of employment, not application. With regard to the proposed list of disqualifiers, AAMVA and some States wrote that States should determine their own disqualifying crimes and could outline those disqualifiers in the DHS certification package. Several States objected to the disqualification of people who have not been convicted on the grounds that such person should be considered innocent until found guilty.

Response: DHS agrees that the time period for interim disqualifications for existing employees should start at the date of employment, not application. DHS agrees that States may supplement the list of disqualifying offenses with their own lists, but those lists cannot replace the Federal list. Finally, DHS agrees that States may make different decisions about whether to move an individual from a covered to a non-covered position even though the individual has not been convicted, and can exercise his or her waiver authority for this purpose under § 37.45(b)(1)(v).

Comment: A few States argued that States should have the option to give employees provisional clearance pending background check results, and that States could outline the procedures for provisional clearance in their certification packages.

Response: As discussed above, DHS believes that it would be a significant security vulnerability to exempt current DMV employees from a background check. DHS has included language that substantially similar background checks (i.e., those that use a fingerprint-based CHRC check and have applied the same disqualifiers as this rule; that include an employment eligibility determination; and that include a reference check) conducted on current employees on or after May 11, 2006, need not be re-conducted.

Comment: One commenter wrote that, of the twenty-nine States that currently carry out some level of employee background checks, only two conduct credit checks. AAMVA and many States objected to the credit check as costly and in conflict with State personnel rules. One State noted that the Equal Employment Opportunity Commission (EEOC) has determined that unless justified by business necessity, it is unlawful to reject candidates based on poor credit ratings.

One State asserted that this requirement is a Federal encroachment into an area historically reserved to States. Some States questioned the link between an employee's financial history and the propensity to commit a crime and posited that implementing this provision as written would cause many union-related issues affecting existing and future employees. Other States pointed out that many law enforcement personnel are not subject to this level of checking. Another commenter objected to the financial check as an invasion of privacy that would not provide useful information, and if DHS requires a financial history check, it should provide standards on how the results of that check should be used by the States

Response: DHS agrees that it would be difficult to make conclusive judgments about an employee or prospective employee's vulnerability to bribery based on a financial history check alone. Since the financial history check would not be determinative, DHS is eliminating the requirement for a financial history check from the final rule.

Comment: AAMVA said that lawful status checks are unnecessary and excessive because States already conduct such checks as part of the hiring process. One State noted that the requirement differs from current Federal requirements for completion

of the Form 1-9. Other States pointed out that SAVE only covers immigrants, not native born Americans. AAMVA and several States noted that lawful status checks are often addressed in union bargaining contracts, and are covered by State personnel laws.

Response: In response to these comments and further consideration of this matter DHS has revised the final rule. Employment eligibility verification using Form I-9 procedures is required for all employees (whether U.S. citizens or aliens) hired for employment at DMVs (or any other U.S. employer) on or after November 7, 1986, REAL ID defines lawful status in a way that is not synonymous with employment eligibility under the INA Thus, the final rule now cross-references current Form I-9 requirements under section 274A of the INA rather than requiring employees to be checked through SAVE. As part of its background check process, the State must ensure that it has fully complied with Form I-9 requirements with respect to covered employees (including reverification in the case of expired employment authorization), but additional status checks are not required. Nothing in this rule in any way modifies any Form I-9 requirement; rather, the background check, if done at a later time than the initial hire, provides another opportunity for the State to check its previous compliance and correct any deficiencies. Form I-9 completion is, of course, required no later than three days subsequent to the first day of employment for all employees.

USCIS operates, in partnership with the Social Security Administration (SSA), an electronic employment eligibility verification program called E-Verify (formerly known as the Basic Pilot program). Participants in E-Verify can query SSA and DHS databases to verify the documentation provided by new employees when completing the Form I-9. States are strongly encouraged to enroll in this program, but, consistent with the

voluntary nature of the E-Verify program as provided by the statutory provisions authorizing the program, it is not required by the final rule.

Comment: One commenter stated that background check processes are flawed, misidentifying people five percent of the time. According to this commenter, in half the States, forty percent of the arrest records have not been updated in five years to indicate disposition of the case. Another State wrote that it would be easier to run checks if they could interface with the FBI database. One State wrote that States should not have to repeat FBI checks if done within the past five years. One commenter asked that the FBI not charge States for accessing their systems.

Response: DHS believes that a fingerprint-based background check is the most efficient way to determine if an individual is subject to a disqualifying offense. FBI checks conducted on or after May 11, 2006 would not need to be conducted again.

Comment: One commenter said that workers subject to a background check deserve a clear and quick process to clear their names and win their jobs back with full restitution of any lost wages. Another commenter suggested that TSA should incorporate provisions from the HAZMAT rules which provide instructions for applicants on how to clear criminal records into the REAL ID rule.

Response: DHS believes that an individual denied employment based on the results of a background check should have the ability to challenge the accuracy of those records. States should make instructions available on how best to contest any inaccurate records or results.

N. State Certification Process; Compliance Determinations

1. Certification Process

Comment: Several commenters requested that DHS receive input and collaborate with States and other organizations on certification guidance and standards. One commenter requested that DHS provide certification packets outlining specific requirements as well as a clear definition of "until all requirements are met." AAMVA and several States recommended that States work with DHS in the development of a streamlined self-certification process to meet the requirements of the Act. One commenter suggested that risk assessment and mitigation plans be included in States' self-certification, and that States participating in the Driver's License Agreement should be able to substitute their compliance review process for DHS audit requirements. One commenter recommended that DHS establish a committee composed of Federal and State officials and representatives of groups which face unique challenges with respect to the REAL ID Act to recommend proposed content for the guidance documents on certification. Some States asked DHS to clarify the requirement for States to provide DHS with any changes to the information requiring certification. Regarding guidance requests, a few States requested a template for the certification document and the security declaration as well as a quarterly reporting standardized format.

Response: DHS has streamlined the certification process, and includes a compliance checklist with this rule. The Material Compliance Checklist will document State progress toward meeting DHS security benchmarks and will serve as the basis for DHS approval of additional extensions until no later than May 10, 2011.

Comment: Several States argued that the certification requirements are too burdensome, citing staffing issues as well as the need for ample preparation time and flexibility to comply with regulations. Similarly, many States argued that the frequency

of certification reporting is too burdensome and questioned the need for quarterly certification reporting. One State recommended a triennial review. Other States thought the requirement to track all exceptions and to notify DHS 30 days before program changes were over-reaching and not authorized by statute. One State recommended that the DHS establish a system of measuring performance instead of recertification.

Response: As documented above, DHS has simplified the certification process.

Comment: Some States suggested allowing States whose DMVs fall under a jurisdiction other than the Governor the ability for the relevant public official to certify compliance. AAMVA and one State argued that the rule should provide that certification be signed by the highest-ranking State official overseeing the DMV, including the DMV Administrator, and not require additional certification from the Attorney General.

Response: DHS agrees that requiring the Governor of each State to personally certify State compliance is too burdensome and has amended the requirement to allow either the Governor or the highest-ranking executive official with oversight responsibility over the operations of the DMV to certify State compliance.

2. Compliance determination

Comment: One State argued that unless and until a State loses a judicial review, it should be considered in compliance. Another State recommended that DHS recognize States that have implemented a number of requirements and plan to continue making substantial progress as compliant. A State asked DHS to allow for the Governor to indicate that the State will remain in compliance until it withdraws from the program. Some States argued that a phased approach was the only viable means to bring States into

compliance. One State recommended that DHS convene a working group with AAMVA to develop a phasing plan for compliance.

Response: As documented above, DHS has adopted a compliance process that significantly lessens the burden of REAL ID implementation on the States.

Comment: Various State and non-State commenters addressed noncompliance issues. One State asked how licenses issued during a compliant period would be treated if a State later fell out of compliance. Another State requested that DHS provide written notification of preliminary non-compliance determination and notice of final determination of noncompliance which would not be effective for 30 business days following receipt. A State indicated it would not agree with non-compliance issues until the standards are clearly identified and agreed upon. One commenter opposed DHS's ability to withdraw a State's certification to issue REAL ID drivers' licenses and identification cards on short notice, noting that decertification would negatively impact truck driver communities, government facilities, and the overall economy of the State.

Response: REAL ID drivers' licenses and identification cards issued when a State was in compliance with REAL ID will remain acceptable for official purposes until they expire, even if the State subsequently becomes non-compliant. The REAL ID certification process will provide a standardized means of measuring and monitoring the DMVs' compliance with REAL ID requirements. DHS will not withdraw a State's compliance on short notice, as certification reporting dates will be established in advance.

Comment: A commenter requested that DHS provide written statements of notice prior to inspections, interviews, or any noncompliance determinations. Some States asked for flexibility and reasonable prior notice when scheduling site visits and REAL ID

compliance audits, in order to have appropriately trained staff available to answer questions and to prevent audit overlaps. Commenters believed that States should have ample opportunity for review and appeal of decisions regarding self-certification.

Response: DHS agrees with these comments. Language has been added to § 37.59(a) to indicate that DHS will provide written notice of inspections, interviews and audit visits. States will be provided with a sufficient opportunity for review and appeal of decisions regarding their self-certification.

Comment: Commenters addressed various training issues. One recommended that DHS allow the current AAMVA fraudulent document recognition training program to be used to meet the REAL ID Act's requirements. This program has been used by States and "is widely recognized as comprehensive, directly related to and easily comprehended by DMV staff." One commenter objected to the requirement for DHS approval of fraudulent document training. Another commenter emphasized the need for ongoing evaluator/authenticator training. Without specific requirements for the training, States lack notice as to whether or not the training will comply with the regulations and will be subject to the unfettered discretion of DHS.

Response: DHS agrees that AAMVA's training program on fraudulent document recognition will be acceptable to meet the requirement of the Act and the final rule. The majority of States currently utilize AAMVA's program.

Comment: One commenter requested a definition of "expedited consideration" of a request for an extension. Other States requested opportunity for input, justification, and consulting in the extension process and assistance with development of the quarterly and annual reports. One non-State commenter requested standards for the issue of

redress, and another suggested that DHS develop standards and plans to audit States' security plans.

Response: The final rule spells out a simple and straightforward process for States to request an extension to the REAL ID implementation deadline. DHS will also allow States to receive an additional extension based on achievement of certain benchmarks established by DHS until no later than May 10, 2011. DHS will notify a State of its determination on a request for extension no later than 45 days of receipt of the request. DHS will work with States and territories throughout the implementation process to assist as required.

The input DHS receives from its stakeholders has been of tremendous value in crafting a final rule that the States may implement and that achieves a greater level of security and confidence in the State-issued drivers' licenses and identification cards. DHS will continue engaging its valued stakeholders to shape the exceptions processes as well as other requirements of the rule.

O. Driver's License and Identification Cards that Do Not Meet the Standards of the REAL ID Act

Comment: One commenter did not agree with DHS that foreign nationals denied REAL ID licenses, even though they are lawfully present but do not yet have the documentation required to demonstrate such status, can simply obtain a non-REAL ID alternative. The commenter wrote that a driver's license increasingly has become a ticket to daily living, and a non-REAL ID license will unfairly and improperly tag the holder as "illegal" and result in discrimination. One commenter wrote that it is not a valid

assumption that most States will issue some other kind of license for immigrants who cannot obtain a REAL ID license. Another commenter wrote that marking non-REAL ID cards would divide the country into two groups and that those with other cards would instantly be suspect and subject to delay, harassment, and discrimination.

One commenter noted that many people such as the elderly or disabled will not need a REAL ID and asked that the State be able to issue a non-compliant identification card to them. By excluding them from the REAL ID process, it will easier for the State to process those who do need a REAL ID within the time allowed.

AAMVA stated that although DHS has argued that States do not have to comply with the Act, the Act and DHS still impose requirements on States for the issuance of noncompliant licenses. AAMVA wrote that this requirement forces States to be in compliance and that the rulemaking goes well beyond Congressional intent in prescriptively outlining State requirements for "non-compliant" REAL ID cards. One State and one individual commenter noted that requiring States to follow these standards imposes a cost on States that choose not to comply, a violation of the 10th Amendment. Another State said that the Federal government cannot require a redesign of documents if the State is not complying. The Federal government should acknowledge the sovereignty of States' rights and respect the traditional State function of licensing drivers.

Response: DHS does not agree that an individual carrying a non-compliant driver's license or identification card from a State issuing REAL ID-compliant drivers' licenses or identification cards would be subject to discrimination. States will make their own business and policy decisions about whether to issue noncompliant cards under 202(d)11 of the Act.

DHS has clarified in the rule that it interprets § 202(d)(11) of the REAL ID Act, which provides requirements for the issuance of drivers' licenses and identifications cards that will not be accepted by Federal agencies for official purposes, as applying only to States participating in the Act that choose to also make these types of documents available. This might apply, for example, to individuals with a religious objection to having their photos taken. DHS does not interpret this section to apply to States that choose not to participate in the Act.

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

Comment: AAMVA, some States, and several additional commenters support the development of REAL ID cards that are WHTI-compliant. AAMVA stated that this is an important direction to ensure the free flow of commerce and travel between the United States and Canada. Some States said that they already collected citizenship data and adding this to REAL ID cards will have little to no additional cost impact.

Several States argued against development of a WHTI-compliant/REAL ID-compliant card. One State said that citizenship is the purview of the Federal government and not that of States, and making a State DMV responsible for verifying citizenship places State employees in a Federal role. This State also noted that citizens with no desire to cross the border will derive no additional benefit from obtaining a REAL ID card that also denotes citizenship. A few States made similar arguments that very few of their residents would find it useful to have a WHTI-compliant REAL ID card. These States also argued that the expense to implement a WHTI-compliant solution would be cost prohibitive.

One commenter emphasized that REAL ID cards must not include citizenship information because of the potential of discrimination against those who choose not to carry a national identification card. Another commenter said that the creation of a dual-use driver's license should be a decision that is made by individuals, after they are fully informed of the benefits, risk, costs, and other details of the programs consistent with the Fair Information Principles.

A few commenters stated that they did not support States listing citizenship information on the REAL ID card or using a REAL ID card as an immigration/border document. These individuals believed that that WHTI-compliant REAL IDs would be significantly more useful to criminals and terrorist and therefore targeted for theft, counterfeiting, and fraud. One individual suggested that DHS could mitigate some concerns that the Department is trying to create a Federal ID by not requiring DMV to denote citizenship on REAL ID cards.

All of the organizations that responded to the question on where citizenship should be listed on the card stated that it should be on the machine-readable zone (MRZ) portion of the card. There were no supporters for listing the citizenship information on the face of the card. These organizations all claimed that placing citizenship information on the face of the card could result in discrimination against the bearer of the card; placing it on the MRZ portion of the card could prevent this from happening.

One commenter described in great detail the need to develop two encrypted MRZs on the card; one zone that can only be accessed and used by DMV and law enforcement officials, and another zone that can only be accessed and used by border and immigration officials. A few organizations commented that placing the WHTI

information on a card may be challenging without increasing the size of the card itself. However, increasing the size of the card would be extremely costly.

Response: DHS welcomes the various helpful comments submitted in response to DHS's questions in the NPRM relating to WHTI. In June 2007, DHS published a NPRM to implement the land and sea phases of WHTI. While DHS acknowledges the desire of some, but not all, States and other commenters to use a REAL ID-compliant driver's license or identification card as a WHTI-compliant border crossing document, DHS did not propose that a REAL ID-compliant driver's license or identification card serve as a WHTI-compliant document in that NPRM and does not propose such in this rulemaking. While the proposed REAL ID requirements include proof of legal status in the U.S., the EDL will require that the cardholder be a U.S. citizen. In addition, EDLs will include technologies that facilitate electronic verification and legitimate movement of travelers through land and sea ports-of-entry.

Comment: A few commenters provided suggestions on the types of business processes and procedures that a State DMV could adopt to create a REAL ID that is also WHTI-compliant. One group suggested that citizens who desire to have a REAL ID that allows for WHTI border entry should be vetted by the State Department in the same manner as a person applying for a passport. The State Department would verify that the individual is eligible to receive WHTI identification and inform the appropriate State DMV that the individual has been approved to obtain a WHTI-compliant REAL ID. The State DMV should create the license/ID card as it normally would and then send it to the State Department to add the WHTI MRZ. There should be two machine-readable zones; one zone would only be able to be used and accessed by law enforcement and DMVs,

and another MRZ that would only be able to be accessed and used by immigration/border officials.

One organization commented that State DMVs will need to be able to utilize the State Department's citizenship adjudication process or create a similar process for adjudicating citizenship.

One State opposed storing citizenship data on the MRZ, preferring to store this information centrally and access it via electronic means.

Response: DHS welcomes the comments submitted concerning potential business practices a DMV could follow to issue both a REAL ID and WHTI-compliant driver's license or identification card, including issues surrounding the adjudication of citizenship for WHTI purposes. As noted above, DHS published a NPRM to implement the land and sea phases of WHTI. At this time, DHS has decided not to incorporate requirements necessary for a WHTI-compliant document into the REAL ID rulemaking.

Comment: Many commenters said that RFID technology, the proposed technology for WHTI documents, should not be used on REAL IDs. Because RFID can be read from up to thirty feet away there are significant privacy and security risks. A few commenters noted that the DHS Data Privacy and Integrity Advisory Committee and the Government Accountability Office both advised against using RFID technology. One organization felt strongly that the use of RFID technology without the use of Basic Access Control and other safeguards would contravene the basic security features that the Department of State has included in new U.S. passports.

Another group believed that States can leverage the same infrastructure that they will need to purchase for REAL ID to incorporate MRZ, proximity chips, and vicinity

chip technology onto a driver's license. The only difference would be the cardstock and the quality assurance processes to ensure that electronics within the card are functioning properly. Another organization suggested that its product can turn the wireless function on or off as needed.

One State suggested that DHS not identify a specific technology to be used, but leave it up to the States to decide.

Response: The use of RFID is essential to the WHTI program in order to ensure facilitation at crowded U.S. land and sea crossing points. Similar concerns are not implicated by REAL ID, which is one of the factors that led DHS to select the 2D bar code as the common machine readable technology on drivers' licenses and identification cards. DHS encourages States to explore alternative technologies on their drivers' licenses and identification cards in order to promote security and technology advances as well as e-government initiatives a State may wish to explore.

Comment: There were several other comments related to the issue of creating WHTI-compliant REAL ID cards. One commenter requested clarification on why REAL IDs themselves would not be sufficient documentation to re-enter the United States. The commenter noted that REAL ID issuance standards require proof of lawful residence status within the United States. and the overall higher standards will make the cards more resistant to tampering and counterfeiting. Therefore, the commenters argued, it may be presumed that a holder of a REAL ID license has the right to re-enter the United States. Another commenter requested clarification on whether "enhanced" driver's license (EDLs) and ID cards that are issued through pilot programs will also have to be REAL ID-compliant. The commenter also requested clarification on how DHS will respond to

States, like Washington State, that have passed legislation refusing to comply with the REAL ID Act unless the Federal government fully funds the State's implementation of the Act.

One commenter requested that DHS consult with tribal governments on how to best implement the REAL ID Act and that DHS consult with tribal leaders on the development of an Indigenous Identification Card for international border crossing.

One individual urged DHS to allow Canadians who are residents of the United States to be allowed to obtain REAL ID/WHTI-compliant drivers' licenses or ID cards, as these individuals make up a significant portion of individuals who cross the border frequently.

Response: DHS acknowledges the desire of some, but not all, States and other commenters to use a REAL ID-compliant driver's license or identification card as a WHTI-compliant border crossing document. In the WHTI NPRM, DHS included a specific discussion of its ongoing efforts with Washington State regarding the issuance and use of an EDL as a WHTI-compliant document. EDLs can only be issued to U.S. citizens since the EDL would serve as the functional equivalent of a passport or passport card at land and sea border crossings. In addition, EDLs must also incorporate the technology specified by DHS to facilitate the legitimate movement of travelers through land and sea ports of entry. With respect to other holders of REAL ID-compliant drivers' licenses or identification cards, any assumption that lawful status as defined for REAL ID purposes equates to a right to reenter the United States is incorrect. For example, applicants for adjustment of status typically must obtain advance parole in order to depart

the United States and lawfully return. DHS has decided not to incorporate requirements necessary for a WHTI-compliant document into the REAL ID rulemaking at this time.

Q. Responses to Specific Solicitation of Comments

Question 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.

Comment: Several commenters did not think the list of documents acceptable for establishing identity needed to be expanded, at least for U.S. citizens, and they were concerned that expanding the list would place a burden on State DMVs. One State did not know of any additional documents that would be electronically verifiable. Another State recommended that the list should not be included in the rule, so that future changes can be easily made. One commenter favored the use of the "acceptable verifiable resource list" of identity documents approved by AAMVA. Another State suggested that the rule should only specify criteria and procedures rather than a list of specific documents for establishing identity.

Response: As noted above, DHS has decided not to alter the list of acceptable documents proposed and discussed in the NPRM.

Comment: One commenter thought that § 37.11 should require non-citizen applicants to provide their alien registration documents so that State officials can compare it to the name on other documents. Various commenters pointed out that foreign applicants would have documents that are not on the list but may have been issued by DHS or the courts to prove immigration status. Some commenters supported other immigration forms, such as Form I-94 (which may indicate lawful status in the

United States) and I-797 (which may be evidence of a pending application). Refugees and asylees are more likely to have these documents before they receive a Form I-766 Employment Authorization Document (EAD). Canadians present in the United States might have these forms rather than a visa. Two States suggested that any document that can be electronically verified through SAVE should be acceptable. Others argued for refugee status paperwork, expired foreign passports if USCIS documentation is current, as well as passports with expired visas and Immigration Court documents. One group recommended that DHS expand the list of acceptable documentation to include family members in the United States on derivative visas. Another group suggested that USCIS consider issuing a temporary refugee photo ID card that could be used to apply for a REAL ID.

Response: State DMVs will use the SAVE system to verify whether an applicant for a driver's license or identification card is lawfully present in the United States. Part of the information required in order to query SAVE is the name of the individual, which can be confirmed through one of the source documents for proving identity. Applicants are free to use any other documentation available, including an I-94 or an I-797, in order to demonstrate lawful status and assist the State in making a SAVE check. DHS also agrees with the commenters who suggested that any document that can be electronically verified through SAVE should be acceptable, since the purpose of providing that document is to prove lawful status, not identity. Neither the I-94 nor the I-797, for example, is sufficient to prove identity. DHS believes that refugees and asylees are issued EADs within a reasonable amount of time such that they are able to obtain REAL ID drivers' licenses and identification cards, and so there is no reason to include other

refugee or asylee paperwork or documentation to the list of documents used to establish identity. Applicants who need an immediate driver's license can obtain a non-REAL ID document from States issuing such cards.

Canadians, however, will need to use their Canadian passport or obtain a U.S.-issued document in order to establish identity for a REAL ID license, as neither DHS nor the States can verify in a timely way that the document has been issued by the issuing agency (a foreign government in this case) as the statute requires. Canadians, however, can typically drive using their Canadian driver's license in the United States and can also obtain a non-REAL ID driver's license from States issuing such cards.

Comment: Some commenters had specific thoughts about the proposed provisions on birth certificates. A State agency suggested that a delayed birth certificate should be specifically named as an acceptable document. Other commenters argued for acceptance of hospital records or baptismal certificates within a year of birth and adoption papers. Another State noted that many births in rural areas are not recorded, and suggested that States should be able to use other documents. Many commenters wrote that the proposed requirement for a certified copy would place a hardship on poor persons and the homeless.

Response: If State law permits the use of a delayed birth certificate, that document can be used by a State. Hospital and baptismal records are not acceptable documents to establish identity, though, in appropriate circumstances, can be used in a State's exceptions process to establish date of birth or lawful status in the United States.

Comment: Two commenters recommended that current State-issued non-compliant drivers' licenses and identification cards and bank-issued credit cards be

included on the list of documents acceptable to prove identity because technology exists to verify and authenticate these documents. Commenters were divided on the acceptance of Native American Tribal Documents, with a few commenters, some Tribes, AAMVA, and two States supporting acceptance of the documents (particularly for birth records), and a few States opposing acceptance of these documents.

Response: DHS does not believe that non-compliant drivers' licenses or credit cards are acceptable documents to establish identity. No identity verification has taken place with respect to these documents. Tribal documents are addressed elsewhere in the responses to comments.

Question 2: Whether the data elements currently proposed for inclusion in the machine readable zone of the driver's license 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?

See full discussion of comments and responses to this question in section I.

Question 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.

Comment: Numerous commenters favored the premise that individuals born before 1935 with established histories should be exempt from the birth certificate verification requirements. Some States added that States should be allowed to establish alternative documents acceptable for ID verification in this circumstance. AAMVA and some States acknowledged that many in this age group may not be able to obtain a birth

certificate or related documents. AAMVA also said that citizens born before 1951 with ten or more years of history with the State DMV and who have passed State-approved verifications should be exempt. Several States said that electronic verification would likely be incomplete and non-electronic verification would be too burdensome for persons born before 1935. Another commenter said jurisdictions should be allowed to segregate the population by risk assessment to enable a managed approach to enrollment in REAL ID. One commenter added that it explicitly proposes using the term "American citizens born before 1935" rather than the term "individuals." A couple of States suggested granting an exemption based on the age of the applicant instead of an exemption based on a fixed date, with one suggesting 62 years of age, based on eligibility to receive social security benefits, for those persons with established histories with the State.

Response: DHS has determined that it will not allow a broad birth certificate exemption for those persons born before 1935, and allows States to accommodate such persons as necessary in their exceptions process.

Comment: States requested clarification regarding "established histories with a State" i.e., whether this means individuals who already have a license or identification card in the State where they are seeking a product. One commenter suggested a history with the State for a minimum period of time, such as twenty to thirty years. This exemption should be part of each State's security plan so risks can be further mitigated through the overall REAL ID plan at the jurisdictional level. A couple of States also said that individuals without established histories should be handled through the State exceptions process, enabling qualified drivers to obtain a compliant license or

identification card. A number of organizations said that these cases should be handled under the State exceptions process. One commenter wrote that DHS should establish a standard to which all States should conform in issuance of birth certificates. Another wrote that the process should be thoroughly documented, reviewed, and updated on an on-going basis. One commenter wrote that the process should substitute some form of identity verification that precludes imposter fraud. Another commenter wrote that this elaborate process is itself another argument in favor of restricting the Federal role in licensing altogether.

Response: DHS has taken a different approach to reducing the number of people that a State DMV must process. DHS consulted with intelligence analysts and experts about how best to target preventive efforts against an individual attempting to fraudulently obtain an identification document to gain access to a Federal facility, nuclear facility, or commercial aircraft.

DHS has determined that, based on information it has reviewed, there is a higher risk that individuals under age 50 will obtain fraudulent identification. As a result, the rule requires States to focus enrollment first on individuals born on or after May 11, 1965 when issuing REAL ID cards. DHS has further determined that there is an acceptable level of risk in deferring the REAL ID enrollment requirements until December 1, 2017 for those individuals who are older than age 50 as of December 1, 2014.

Comment: Two States said that customers born before 1935 should make every attempt to comply with REAL ID rather than being granted a blanket exemption. If compliance is not possible, exceptions procedures (along with other documents to reasonably prove identity) should be the next step.

Response: DHS agrees with these comments and has decided not to adopt an exemption for individuals born before 1935, as discussed above.

Comment: AAMVA and several States said that individuals born before 1935 should not only be exempted from the birth certificate requirements, but also wholly exempt from the entire enrollment process since these individuals do not pose any potential threat. However, one State said it lacks the expertise to opine on the risk of terrorism this exemption would pose.

Response: As noted above, DHS is not proposing to exempt any individuals from the REAL ID enrollment process.

Comment: Other commenters suggested the following exemptions from reenrollment: individuals for whom proof of identity, residency, lawful status and SSN can be proven electronically, and citizens who are elderly, disabled, in nursing homes or mental institutions and who will not be getting on an airplane or entering a Federal facility.

Response: As noted above, DHS is not proposing to exempt any individuals from the REAL ID enrollment process. DHS urges States to make appropriate accommodations for handling the elderly, disabled, and those in nursing homes or mental institutions. Section 202(d)(11) of the Act gives States the opportunity to issue non-compliant licenses that are not accepted for official purposes and may not necessarily require an in-person enrollment, depending on the State's issuance process.

Question 4: If a State chooses to produce drivers' 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.

See full discussion of comments and responses to this question in section P.

Question 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.

See full discussion of comments and responses to this question in section I.

Question 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.

Comment: AAMVA listed ten criteria for measuring a State's progress towards implementation of the REAL ID requirements – procurement practices, process changes, contractual arrangements, funding, legislative authority, personnel, facilities, computer systems, new verification systems, and existing verification systems. Some States suggested variations on these themes, proposing that a set of standardized benchmarks was not realistic. Rather, each State should be able to determine appropriate benchmarks depending on what they had to do to implement REAL ID. Progress could be measured against implementation plans States submitted to DHS and should be based on a phased approach. One State suggested that DHS create a matrix that could be used to show progress for the major components of REAL ID. Another State argued that it is difficult to establish benchmarks before all regulatory requirements have been finalized. One State recommended a "strategic" rather than "prescriptive" implementation approach.

One privacy group stated that the final rule must include robust security standards for national querying systems. A vendor association provided detailed recommendations on access control and authentication practices. One State made very detailed recommendations on privacy standards including a pre-defined audit requirement. A vendor association recommended strong sanctions for violations of procedures to deter the insider threat and notification of anyone whose information is breached.

Response: The final rule specifies the elements necessary to be REAL ID-compliant, and DHS has proposed a checklist process for States to demonstrate completion of certain compliance benchmarks, and full compliance with the Act and these regulations.

Question 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.

See comments and responses to this question in section M.

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

Comment: Several States indicated that individuals from American Samoa and the Commonwealth of the Northern Marianas should be issued a REAL ID if they provided acceptable documents like birth certificates, valid passports, unexpired driver's license, or U.S. issued immigration documents.

In addition, a few States supported an exception process for these territories. One State said that without Federal funds, it would be difficult if not impossible for both territories to comply due to complexity, cost and timing issues. Some States questioned

whether American Samoa would be able to issue drivers' licenses and identification cards under the REAL ID Act and regulations. Other States claimed that without evidence of U.S. citizenship, Northern Marianas residents would not be able to obtain a license or card. One State recommended that DHS accept the Northern Mariana Card (I-873) to establish identity and residency. Customers without this card could be assisted under current State exceptions processes. Another State also suggested acceptance of the Re-entry Permit/Refugee Travel Document (I-327, I-571).

AAMVA and some States requested clarification as to the specific issue caused by these groups of applicants.

Response: DHS believes that American Samoa and the Commonwealth of the Northern Marianas will be capable of complying with the REAL ID requirements in the same time frame as other States and Territories.

Question 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.

Comment: See comments and responses to this question in section I. Also, AAMVA commented that States will face significant contractual conflicts if the document security standards in this NPRM remain in the final rule. States are using the AAMVA Driver Licensing and Identification Card Design Specification as the model to prepare bid packages for new contracts or renewals. Contract periods for card vendors vary by State and are driven by procurement rules. One State, for example, has a contract in place for the next seven years. Most States have at least five year contracts. AAMVA recommended that DHS use the AAMVA Driver Licensing and Identification Card

Design Specification as the minimum card security standard, allowing States to build on its provisions. States should not be expected to break or amend existing contracts and should not be expected to implement any changes to card security until their existing contracts expire.

Response: See comments and responses to this question in Section I.

Question 10: The Federalism aspects of the rule, particularly those arising from the background check requirements proposed herein.

Comment: Several commenters said that REAL ID was beyond Congress's enumerated powers because the States have a valid immunity claim. Another commenter wrote that REAL ID usurped States' traditional authority. One commenter wrote that it is a violation of the tribal-Federal relationship to require a tribal government official to go to a State government official in order to obtain proof of identification in order to travel and conduct official tribal-Federal government business. One commenter said that State DMVs cannot revoke licenses or identification cards issued by another State. One State found no Federalism issues as States are able to control the design, and, potentially, the security features of its cards. However, other States voiced a number of Federalism concerns.

One State presented a list of impacts flowing from the REAL ID program: procurement practices, process changes, existing contractual arrangements that cannot be altered without significant penalty, fund appropriations, laws, facilities, computer systems, requirement of new verification systems. Similarly, some States argued that the REAL ID regulation could not survive a challenge brought under the 10th Amendment of the Constitution. It continued, "Given an affidavit issued by the Governor of the

Commonwealth, DHS would have universal, unfettered access to employees and systems that are dedicated to a traditionally State function." Another State wrote that DHS should not intrude into the traditional State function of licensing drivers and issuing identification cards by attempting to prescribe the processes for creating, issuing, and administering REAL ID cards, and that DHS should specify the security, performance, and quality characteristics that REAL ID participating jurisdictions must achieve. Some commenters believed that the REAL ID Act violates both the spirit and the letter of Federalism law. The commenters wrote that the REAL ID Act aims to conscript the States into creating a national ID system, and that it is "this kind of scheme" that the Framers expected Federalism to guard against. Because of this, many States have passed anti-REAL-ID resolutions and legislation.

Response: The REAL ID Act provides the Secretary of Homeland Security with authority to issue regulations. DHS understands that there is a balance between Executive discretion in interpreting the REAL ID Act through regulation, while also respecting the States' autonomy to govern an inherently State function – the driver's license and identification card issuance process. DHS has attempted to preserve State autonomy wherever possible, while remaining consistent with the Act, and believes these regulations represent a logical interpretation of the Act and Congressional intent.

Comment: One commenter argued that States should have discretion to determine whether to conduct background checks on State employees. One State DMV said that because it conducts a fingerprint-based background check on its employee-applicants, implementing the REAL ID requirement would have "minimal" impact. In contrast, one State said that in requiring a background check for State employees, DHS is

"overreaching." Because the requirement includes several checks, only one of which a DMV could use to disqualify an employee from performing certain REAL-ID-related activities, a State argued that the rule impacts both the individuals a State may hire and retain in certain positions. It also requires a collection of information for no stated reason. Another State DMV wrote that DHS goes beyond the statutory language in requiring a background check, and suggested that DHS strike the provision.

With regard to the financial history check, one State noted that this aspect of the draft regulation would intrude into the relationship that State governments have with their employees. It argued that DHS could avoid Federalism issues by having its regulations "express the security characteristics that a State would need to achieve rather than prescribe how State processes should operate." The Federal government, it said, should not regulate hiring practices for State employees. One State wrote that it has discontinued credit checks because it was not an adequate indicator of a person's behavior or ethics.

Response: As noted above, DHS believes it has the authority to require background checks. Based on the comments received, DHS has decided to eliminate the financial history check of DMV covered employees and prospective employees.

Comment: Although one State agreed that DHS has authority to review State compliance within the scope and criteria of the auditing granted by the statute, this State asserted that DHS exceeded the scope of its authority in promulgating § 37.59(a), which lacks a check on seemingly unlimited Federal authority to inspect State processes.

Response: DHS does not believe the language of § 37.59(a) provides DHS with unfettered authority to oversee the actions of State government. Indeed, the section

provides the opportunity for States to challenge a DHS determination of non-compliance, rather than a Federal authority with no right of appeal. DHS has also relaxed the reporting requirements in this final rule in response to comments that the reporting requirements in the NPRM were too burdensome.

Comment: One State asserted that it is beyond DHS's authority to compel non-participating States to maintain a motor vehicle database with the minimum required REAL ID information and to share access to any such database with other States.

Response: DHS is not compelling non-participating States to meet any of the requirements of these rules.

Comment: A State objected to the requirement that a REAL ID cardholder's address change requires the person to report and document the change in person at a DMV office. The State says it is apprehensive that the proposed rules erode the important principles of Federalism, especially regarding managing elections. When a driver applies for voter registration, the State automatically checks to see whether the address given on that card is the same as the address on a State-issued driver's license or identification card. If there is a mismatch, State law requires automatically changing the license or identification card address to match that on the voter application form. This State requested that DHS give serious consideration to allowing this automatic updating practice to continue. Another commenter said DHS should ensure that the final regulations continue to provide States maximum flexibility to determine which employees are subject to the requirements of this section.

Response: As noted elsewhere, the final rules do not require an individual to have an in-person transaction with the DMV to change their address.

Comment: One commenter said that because direct regulation of the States would be unconstitutional, the REAL ID Act inappropriately conditions Federal acceptance of State-issued identification cards and drivers' licenses on their meeting certain Federal standards. The commenter was also concerned that DHS was using State machinery to implement a Federal program. However, the commenter asserted that it is within Federal power for DHS to condition acceptance of identification cards and drivers' licenses on priorities closely related to national security, including meeting standards for privacy and data security.

Response: Congress passed the REAL ID Act to implement a recommendation of the 9/11 Commission Report to increase the security, credibility and confidence in identification documents. Congress, in drafting the law, and understanding the Constitutional concern of directly regulating the States, made the law binding on Federal agencies in specifying that only REAL ID-compliant drivers' licenses would be accepted by Federal agencies for official purposes after the law is implemented. DHS agrees with the commenter that the Federal government has the authority to condition acceptance of drivers' licenses and identification cards on the meeting of certain standards and requirements as defined in the REAL ID Act and the implementing regulations.

Comment: One commenter concluded that Congress and DHS could have supported meaningful Federalism by supporting States' pre-REAL ID initiatives to produce an interstate compact to achieve interoperability of State databases.

Response: This comment is outside the scope of the rulemaking.

Question 11: How the Federal government can better assist States in verifying information against Federal databases.

Comment: Several States and other commenters had a number of suggestions including the following:

-- Develop and test or enhance Federal databases to meet States' needs.

-- Establish standards for system performance and connectivity.

-- Ensure that matches can be made with as little manual intervention as possible.

-- Establish standard naming conventions.

-- Put security standards in place.

-- Fund system development and assist States financially in performing verifications.

Response: DHS is collaborating with its Federal partners, AAMVA and the States to design and implement verification systems to support the requirements of the REAL ID Act and regulations. DHS is working on improving the reliability, usability and accuracy of existing systems like SSOLV and SAVE to meet States' needs to minimize the manual intervention necessary.

In addition, DHS will work with DOT, AAMVA and the States to reinforce the security and privacy features of this communications and systems architecture to include practices consistent with fair information and Federal Information Security Management Act principles. In partnership with DOT, AAMVA, and the States, DHS will issue best practices to guide future systems design, development and operation. DHS is also working with Federal, State, and nongovernmental organizations to identify and improve name formats and matching algorithms used by identify verification

Question 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.

Comment: Several commenters wrote that REAL ID will decrease identity theft. Several other commenters thought that a decrease in theft might not be attributed to REAL ID but be due to the fact that many States are implementing more stringent rules for obtaining a driver's license.

A few commenters claimed that REAL ID will have little to no impact on identity theft. One commenter noted that most instances of identify theft are a result of a stolen social security numbers or credit cards, and that REAL ID does not address these types of thefts. Another organization stated that "loopholes" in the source documentation requirements for those without a permanent addresses or birth certificates take away any perceived REAL ID benefit.

Most of the commenters thought that REAL ID would increase identity theft. Commenters wrote that the NPRM did not propose sufficient protection and security controls to ensure that the information being collected and stored will be immune to theft or misuse. Several commenters said that the databases storing digital images of social security numbers, bank statements, and birth certificates will be an identity-thief's dream target. These images, once in the hands of criminals, will be easy to counterfeit. If systems are linked, a single breach in security will potentially compromise 240 million individuals. Several commenters also highlighted that threat to this information may come from within DMVs. One organization quoted that over 100 million records of U.S. residents have been exposed due to security breaches.

Response: DHS provided a detailed analysis on the ancillary benefits of the proposed rule on REAL ID. We noted, as the comments suggested, that the proposed

rule may have only a small impact on reducing identity theft. REAL ID will only have the ability to impact those types of identity theft that require a drivers license for successful implementation and only to the extent that the rulemaking leads to incidental and required use of REAL ID documents in everyday transactions, which is an impact that also depends critically on decisions made by State and local governments and the private sector. With the current costs of identity theft being high, we believe that even if the ancillary benefits associated with identity theft are low, when these benefits are combined with other benefits of this rulemaking, that this rule is cost-beneficial.

Many commenters believe that REAL ID would increase identity theft. We find, at the current time, that it would be difficult to draw any conclusions such as this since the effort or cost to individuals to obtain and use a passable fraudulent identification card is expected to be much higher than it is at present. Only those people who believe that they will reap substantial benefits would be willing to incur the cost of creating and using a fraudulent identification card.

With regard to the general comment that REAL ID is expected to reduce instances of underage drinking through the use of false/fraudulent identification, DHS believes that REAL ID may reduce on the margin the rate at which underage drinking occurs. The rate at which it does so partly depends on State and local authority and/or private employer decisions as to what form of identification is acceptable for particular purposes, and the effectiveness with which identification checks are implemented. DHS is not willing to quantify, at this time, the expected benefits that would be achieved from a reduction in underage drinking.

Comment: Regarding the ancillary benefits of REAL ID, some States supported DHS's suggestion that REAL ID could reduce underage drinking and purchase of cigarettes by making it easier for vendors to identify fake identification cards. Other commenters wrote that REAL ID could also promote highway safety by allowing law enforcement officers to process vehicular accidents and traffic citations faster and more accurately, and potentially aid other law enforcement efforts.

Several commenters noted that one of the possible ancillary effects of a REAL ID is that commercial entities will be able to market to individuals without the individual's permission. The MRZ and the 2-D barcode technology discussed in the NPRM makes it easier for third parties to obtain sensitive information about the holder of the cards. Several commenters gave examples of how commercial entities will make REAL ID the default document for everyday transactions and thus will be able to obtain, store, and track individual's age, address, and purchases.

Three organizations noted that State transactions, such as the issuance of professional/occupational licenses (for example, licensing for doctors, lawyers, nurses, real estate brokers) and hunting and fishing licenses, could be done with a higher level of assurance that the license is being given to the right person. Two other organizations also said that health-related and financial companies would also receive security benefits associated with more trust in the validity of the identification cards. One commenter stated that all employers would benefit because they would be better able to determine employment eligibility.

Response: DHS believes that the potential ancillary benefits of this rulemaking would be in many areas. Should acceptance of REAL ID cards become widespread, such

ancillary benefits may include reduction in fraudulent access to public subsidies and benefits programs, illegal immigration, unlawful employment, unlawful access to firearms, voter fraud, underage drinking, and underage smoking. DHS believes that REAL ID may reduce on the margin, the rate at which these fraudulent activities take place. The degree to which they do so will partly depend on State and local authority and/or private employer decisions as to what form of identification is acceptable for particular purposes, and the effectiveness with which identification checks are implemented. DHS cannot, at this time, measure these benefits quantitatively.

With regards to organizations, businesses, etc., DHS is not preventing the use of REAL ID in State transactions and the individual who is having the document presented to him can place any level of trust he/she wants in the REAL ID document.

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

Comment: A State recommended that DHS seek out U.S. EPA or a similar group to evaluate the potential environmental impacts. One State DMV wrote that the environmental impacts of the rule would be minimal. States may have to perform the required environmental impact analysis if changes to issuance facilities are necessary. AAMVA suggested that environmental impacts associated with retrofitting the facilities to meet physical security standards will result in some environmental risks such as asbestos removal.

One State asserted that the increased visits by individuals to renew their licenses and corresponding activities associated with creating a license (for example, increased

usage of electricity, scanners, copiers, printers, and paper) will impact air, ground, and water quality, and result in unnecessary waste disposal and consumption of natural resources, electricity, and other fuels and add to traffic congestion. This State recommended that DHS revise the rule to employ a phased approach which could allow States to certify and renew on schedules that will not adversely impact the normally occurring renewal cycle.

One commenter suggested that the durability provided by longer life drivers' licenses and identification cards could result in less material going into the waste stream resulting in an environmental benefit.

Response: DHS carefully evaluated those comments along with other potential environmental impacts of this rule. The comments show that, if the States choose to create a REAL ID process, any potential environmental impacts which might be significant, can be mitigated. DHS concludes that the rule's potential impacts are minimal and notes that the rule does not force an immediate action but only lays the foundation for subsequent action. If States seek follow-on DHS grant funding, approval, or other activity for implementation of the rule, then the potential environmental impacts associated with the follow on activity must be reviewed.

Question 14: Whether other Federal activities should be included in the scope of "official purpose."

See comment and response to this question in section B.

Question 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 drivers' licenses.

Comment: Most commenters supported the "one driver, one record concept," and most States said Federal funding for an "all drivers" system would promote the concept. A couple of States specifically endorsed DRIVerS (Driver Record Information Verification System). Many States joined AAMVA in endorsing a State's initiative to enter into a Driver License Agreement to develop "a nationwide pointer system with the driver record and driver history transferred to a 'change State record' when the driver moves to a new State." AAMVA and many States also endorsed basing any such pointer system on the Commercial Driver License Information System (CDLIS).

One State said that any "all drivers" verification system must include "reciprocity rules" so that an individual who is required to move frequently across States need not undergo a complete REAL ID check every time. However, one commenter said a CDLIS-type system is a concern because it is a "one person one license (or ID card) one record system" with no regulatory or statutory limitations on who can access information and for what purpose. To protect privacy and ensure driver safety across States, the commenter said the existing Problem Driver Pointer System/National Driver Register is better.

A few commenters also joined AAMVA in endorsing the AAMVA/National Highway Traffic Safety Administration joint initiative to develop a digital image exchange project to identify multiple State license holders. Some States echoed a comment from AAMVA that because a driver's license applicant must surrender his or her current license from another State as a condition of receiving a new license, the States already follow a policy of one driver, one license. Another State said that States should require a driver's license applicant to self-declare the existence of a prior compliant or

non-compliant license or card and require confiscation and notification to cancel before the new State issues a document. Several commenters endorsed using the Driver License Agreement compact as an extant system for promoting "one driver, one record."

Other process recommendations included the suggestion that a national business process standard be developed to let jurisdictions know of the theft or loss of a REAL ID card and forming an agreement similar to the DLA that both REAL ID and non-REAL ID States can use to ensure cross-checking before a jurisdiction issues any driver's license. Requiring "cleaning" of existing databases and comparing legacy databases used to issue a REAL-ID compliant card was also recommended.

One commenter said that having only one license for multiple purposes would better promote the concept than having non-REAL ID and REAL ID drivers' licenses. It also said that the United States must accept standards nationwide to be used with confidence of driver's license exchange to move across boundaries and should encourage/mandate reciprocity of like licenses.

Some commenters noted problems with implementing the "one driver, one record" concept, stating that, without participation by all States, the system is fundamentally flawed in that a person could hold multiple non-REAL ID driver licenses and a REAL ID-compliant card. One State said that DHS lacked authority to compel a non-REAL ID State to participate in systems that promote the concept. It suggested that the "one driver, one record concept" should only apply to the REAL ID-compliant system.

Other States said the rules should allow a person to hold both a REAL ID-compliant card and a non-REAL ID card in any combination "with the limitation that a

driver has no more than one license and one card at a time." One State suggested that a person not hold more than two REAL ID-compliant cards at a time: a driver's license and an identification card. This commenter said a person might wish to carry a REAL ID-compliant card and keep another at home. One State said that it issues identification cards to individuals who may hold a license in another State.

Some States said that DHS's proposal and the REAL ID Act impede "one driver, one record." That would happen, these commenters said, where these authorities require "a State DMV to take measures to confirm that an applicant has terminated or has taken steps to terminate a REAL ID driver's license or identification card issued in another State." One State proposed that DHS change § 37.33(c) to state that a person who applies for a REAL ID in his or her State of residence has "taken steps to terminate the prior card." One State wanted to know how DHS would define "terminate."

One State said that because there is no system through which a State could check whether a person already holds a REAL ID driver's license or identification card in another jurisdiction, DHS should eliminate the requirement that States must make such a check. Another State asserts that such a capability should exist now across all fifty States.

Several commenters remarked on the use of technology to promote the "one driver, one record" concept. One commenter endorsed smart card-enabled REAL ID documents requiring a one-to-one match. A consulting group described a biometric identifier as the only known manner to prevent one individual from procuring more than one license or identification document. This commenter said DHS should identify and

standardize a suitable biometric property and create a privacy-sensitive solution for performing the necessary biometric comparisons.

One commenter said that DHS should have presented and analyzed in detail different architecture models (other than CDLIS) for the system States can use to check whether a REAL ID applicant already holds a REAL ID card issued by another jurisdiction. Noting that a system promoting "one driver, one record" must promote privacy, security, and accuracy, another commenter said CDLIS is not a federated query system, but a national database. It commented that simply scaling up this system will not establish a federated query service, but will create a national ID.

One commenter wrote that it is concerned about DHS's failure to articulate what defines a person's unique driver's license or identification card number; the proposed rule is silent on the form this unique number will take and does not specify whether the number will be unique nationally or solely within a single State.

Response: Section 202(d) of the REAL ID Act prohibits States from issuing REAL ID cards to a person who holds a driver's license in another State without confirmation that the person has terminated, or is taking steps to terminate, the other license. We have amended this final rule to clarify this statutory requirement. See § 37.33. DHS supports the concept of one driver, one license. DHS is not, however, authorized under the REAL ID Act to use this final rule to prohibit States from issuing non-REAL ID driver's licenses to persons who hold licenses in other States or to find that a State is not in compliance with the minimum standards of the REAL ID Act if such State issues driver's licenses to persons holding licenses in other States. DHS is limited

under its authority in the REAL ID Act to prohibiting States from issuing REAL ID cards to persons who hold licenses in other States or who hold another REAL ID card.

Question 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.

Comment: A few States said that although a REAL ID should be recognizable as such, a standardized appearance would facilitate counterfeiting. Another State suggested that States should only have to mark REAL ID-compliant cards, not mark non-compliant cards. Other commenters supported the use of an identifier for non-compliant licenses and cards, as DHS would need a mechanism to tell if a license issued before the Act was compliant. NGA recommended placing a restriction code on the front of the license with text on the back to denote whether the license was REAL ID-compliant. AAMVA, several States, and another commenter all argued against standardizing a unique design or color for the non-Real ID cards. Some commenters wrote that DHS had no authority to require States to adopt a standard design or color for the non-REAL ID cards, citing Federalism. One commenter wrote that mandating distinct designs or colors for both REAL ID and regular license and ID cards and requiring non-REAL ID drivers' licenses to have an "invalid for Federal purposes" designation turns the voluntary card into a mandatory national ID. Several also expressed concern that standardization would make counterfeiting of the cards easier, since counterfeiters would only have to focus on one document. The consequences of successful counterfeiting would be more severe, they said, since the whole system would be compromised and all States would then have to change their cards. Some commenters said that diversity in security features, as long

as they met a common performance standard, would be best. Commenters said that a standardized design would increase the perception that a national identification system was being created.

Response: While cards that do not satisfy the requirements of the Act must clearly state on their face that they are not acceptable for official purposes, DHS is not mandating a specific design or color for such cards. DHS agrees with States that recommended marking compliant cards and as such, requires compliant cards to be marked with a DHS-approved security marking.

Comment: Many commenters opposed a REAL ID standard design. One commenter wrote that requiring a single standard configuration will limit the ability of jurisdictions to adapt to changing threats in their particular environment and could drive up costs unnecessarily. Many States expressed concern about increasing the threat and consequences of counterfeiting. Several States said they should be allowed to continue to use unique designs for their drivers' licenses and ID cards (one noting it held great value for State identity), while others argued that States should be allowed to maintain control of the design of their licenses to the greatest extent possible. AAMVA noted that its current Card Design Specification does not require a similar color for all States, although it standardizes security features. AAMVA recommended that "branding" be applied to the REAL ID, but it also recognized that this would lead some individuals to believe this was a step toward a national ID card. State commenters wrote that a benefit of a standard color would be to ease training of screeners and help ensure that screeners could easily identify a compliant REAL ID-compliant card.

One commenter wrote that REAL ID should mandate a standardized color or design. However, other commenters wrote that DHS should not mandate a standard design or color, that a standard design is not authorized by the REAL ID Act, that a standardized design is strictly prohibited by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, and that a uniform REAL ID design would be an "enormous" security risk.

Response: DHS is not mandating a single design or color for REAL ID-compliant drivers' licenses or identification cards, and recognizes a State's right to have a unique design. However, in response to several commenters, DHS is requiring that cards issued in compliance with REAL ID be marked with a DHS-approved security marking.

IV. 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 rule contains the following new information collection requirements. Accordingly, DHS submitted a copy of these sections to OMB for its review. OMB has not yet approved the collection of this information.

This final rule will require States participating in the REAL ID program to meet certain standards in the issuance of drivers' licenses and identification cards, including security plans and background checks for certain persons 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). This rule will support the information needs of: a) the Department of Homeland Security, in its efforts to oversee security measures implemented by States issuing REAL ID drivers' licenses and identification cards; and b) other Federal and State authorities conducting or assisting with necessary background and immigration checks for covered employees.

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).

DHS estimates that each State will submit a certification of compliance or request for extension, together with a security plan. Subsequently, each State will be required to re-certify its compliance with the REAL ID Act every three years on a rolling basis. As part of the certification package, States will be required to submit 1) a copy of their security plan; 2) their documented exceptions and waivers procedures; and 3) a written report on card security and integrity (which must be updated whenever a security feature is modified, added or deleted). DHS estimates that States will spend approximately 42,000 burden hours in the first year to complete the certification requirements. DHS projects that the burden hours will rise to 56,000 hours annually in subsequent years. DHS estimates the cost to the States will be $1.11 million in the first year and $1.48 million every year thereafter, for an annualized cost estimate (over three years) of $1.35 million.

States must subject covered employees to a background check, which includes a name-based and fingerprint-based criminal history records check (CHRC). DHS estimates States will incur costs for employee background checks of $1.44 million in the first year, $0.61 million in the second year, and $0.37 million in the third year, for an annualized cost estimate of $0.80 million.

Finally, States must maintain photographs of applicants and records of certain source documents. DHS estimates that States will incur 2,275,000 hours for information technology (IT) in the first year, and 348,000 hours in subsequent years, for an annualized hour burden estimate (over three years) of 990,333. DHS estimates that ten percent of all IT costs is related to the recordkeeping requirements. Thus, DHS estimates that out of a total one time cost of $601.9 million for all State systems, ten percent, or $60.2 million, will be incurred in the first year, and $9.3 million in the second and third years as a result of this collection of information, for an annualized cost of $26.26 million.

DHS received no comments directed to the information collection burden.

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. First, Executive Order 12866, Regulatory Planning and Review (58 Fed. Reg. 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, it explicitly stated that the REAL ID Act is binding on the Federal government, and not the States. 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." Thus, as a matter of law, the UMRA requirements do not apply to this final 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 detailed Regulatory Evaluation placed in the public docket.

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 economically

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 requirements finalized by this rule. A complete regulatory impact assessment, as required under Executive Order 12866 and OMB Circular A-4, will be set forth in a separate document in the docket for this regulatory action at http://www.regulations.gov at Docket Number DHS–2006–0030. The details of the estimated costs and benefits, including potential ancillary benefits realized by the requirements set forth in this rule, follow the A-4 Accounting Statement. The uncertainty analyses are being recomputed and will be published in the forthcoming final regulatory impact assessment.

The Department of Homeland Security (DHS) is conducting a Regulatory Evaluation of the benefits and costs of the final minimum standards for State-issued drivers' licenses and non-driver identification cards pursuant to the REAL ID Act of 2005. These standards will impact the lives of approximately 240 million people and the operations of all 56 State and territorial jurisdictions.

Assumptions

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

- Years One through Four – the three and one-half year period from January 2008 to May 11, 2011 during which States will have time to make the business process changes and investments to meet the standards of REAL ID. In addition, States meeting the interim standards of Material Compliance with

the rule must begin enrolling their populations in REAL ID beginning no later than January 1, 2010.

- Years Four through Eleven – the seven year period during which States will continue and complete enrollment of their populations in REAL ID. States will begin issuing fully compliant REAL ID licenses no later than May 11, 2011. Moreover, DHS has adopted an age-based approach to REAL ID enrollment. By December 1, 2014 all individuals born on or after December 1, 1964 (that is, 50 years of age or under) will be required to present a REAL ID if they use a State-issued document for official purposes. Thus, individuals born on or after December 1, 1964 will have a minimum of four years to obtain a REAL ID. Individuals born before December 1, 1964 will have an additional three years to enroll before the final enforcement deadline of December 1, 2017.

The final rule incorporates significant changes to the Notice of Proposed Rulemaking. As a result, we have revised some of the assumptions upon which the original Regulatory Evaluation was based. The revised assumptions are detailed below:

1) That all States will comply in accordance with the revised timeline.

DHS recognizes that most, if not all States will be unable to comply by May 2008 and will file requests for extensions that will result in compliance implementation schedules that could mitigate some of the startup costs examined below. Hence, the costs allocated to the period prior to May 2008 will be redistributed to subsequent years.

2) That 75 percent of the nation's DL/ID holders will seek a REAL ID credential.

The original NPRM assumed that 100% of the candidate population would seek to obtain REAL IDs. This assumption was combined with two additional assumptions, namely that:

1. States will not require all individuals to obtain a REAL ID;
2. Some States will continue to issue non-compliant licenses along with REAL IDs

The Department has reviewed the 100% assumption and concluded that it is unrealistic in light of the latter two assumptions. If States do not require all applicants to obtain REAL IDs, it is highly improbable that 100% of the population will apply. It is difficult to cite any example of a truly voluntary course of action that results in 100% compliance. If States offer a choice of either compliant or non-compliant licenses to applicants, some portion of the population will choose to receive a non-compliant license because:

1. They do not need a REAL ID for Federal official purposes
2. They already possess a substitute document – for example, a U.S. passport – that will serve the same purpose as a REAL ID

Thus, the Department has reconsidered and eliminated the assumption that every individual 16 or older will seek to obtain a REAL ID within the timeframe of this analysis.

The difficult question, therefore, is what level of participation in REAL ID can be realistically expected? What should be the primary estimate for participation by the American public in REAL ID?

The Regulatory Evaluation utilizes a primary estimate of 75% based upon the following analysis:

1. A significant number of States will not require that all residents seeking drivers' licenses or identification card obtain a REAL ID. Eight states currently issue licenses to individuals who cannot demonstrate lawful states and a significant number of States are likely to make REAL IDs an option.
2. 25% of the population already holds a valid passport and the Department of State anticipates that this figure will increase to approximately 33% in the next few years.[3] Individuals with valid passports do not need to obtain a REAL ID as passports are likely to also be accepted for the same official purposes (i.e., boarding commercial aircraft) as a REAL ID.
3. 20% of the population has never flown on a commercial airplane and 47% flies "rarely or never." [4] This second group is unlikely to need a REAL ID and members of this group are highly unlikely to belong to the group of valid passport holders.
4. These two groups, combining to constitute a group of at least 40% of the population, should not need to obtain a REAL ID as acceptance of identification for official purposes. Assuming that a large proportion of this group will seek to obtain a REAL ID regardless of imminent

[3] Testimony of Maura Harty, Assistant Secretary of State for Consular Affairs, before the Senate Foreign Relations Committee, International Operations and Organizations Subcommittee, June 19, 2007, at http://travel.state.gov/law/legal/testimony/testimony_806.html.
[4] Statistics reported in The Airline Handbook, issued by the Air Transport Association and located at http://members.airlines.org/about/d.aspx?nid=7954 and by the Gallup Organization at http://www.gallup.com/poll/1579/Airlines.aspx.

need, we believe that 25% of the candidate population will not seek to obtain a REAL ID.

3) States will issue both REAL IDs and non-REAL IDs.

DHS anticipates that States will offer an alternative DL/ID (not acceptable for official purposes) to those who are unwilling or unable to obtain a compliant one. A number of States issue or plan to issue licenses to individuals that cannot document lawful status. Other States are expected to allow individuals to hold both a driver's license and identification card. Finally, a number of States have evaluated or expressed interest in offering REAL IDs as an additional, voluntary license. 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 drivers' licenses and identification cards, thereby reducing their operational and system costs.[5]

4) That all IT systems will be functional by May 11, 2011.

The NPRM assumed that all IT systems would be functional by May 11, 2008. DHS now recognizes that this assumption was overly optimistic. Therefore, DHS has extended the deadline for compliance with the rule until May 11, 2011 to give the States, Federal agencies, and non-governmental organizations like AAMVA the time to complete the communications and IT infrastructure needed to implement REAL ID. Therefore, DHS has recalculated the costs assuming that all required verification data systems be operational and fully populated by May 11, 2011, the deadline for full compliance by States. DHS is working to bring these systems on-line and up to standards as soon as possible and will work with the States to develop alternative procedures.

[5] Eight states currently issue licenses to undocumented immigrants and will- most likely – continue to do so. These States are: Michigan, Maryland, Hawaii, New Mexico, Oregon, Utah, Washington, and Maine.

5) That 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 will incur lower compliance costs than other States.

6) The typical validity period of driver's licenses in a given State is the validity period for all DL/IDs in that State.

DHS is aware that within a State DL/IDs often have varying validity periods but was unable to determine how many people held each of these varying types of credentials and when they were issued. (For more details, see the discussion of Validity Periods in the Status Quo section.) Also, the final regulation creates a one-year license for certain aliens. DHS was able to determine that some people already hold such licenses, but not *how many* people hold them. DHS was also unable to determine how many people will hold them under the REAL ID rule. While this methodology has limitations, using the typical validity period of DL/IDs was the most reliable method available to estimate future issuances.

7) Those drivers who would be required to comply later in the issuance cycle will take advantage of this delayed compliance.

DHS has computed the costs for the over age 50 drivers by moving that segment of renewals towards the 2017 deadline. DHS assumes the distribution over time for renewals is similar to the rest of the population. Therefore these license renewals are not bunched up but entered as the same distribution as other drivers but with the last of the pool completing in 2017.

8) The cost of lost/stolen DLs/IDs and central issuance is included in the cost of this final rule.

The regulatory evaluation for the proposed rule assigned the cost of having to replace a lost or stolen legacy ID with a REAL ID as being a regulatory compliance cost. This means that if an individual loses his/her legacy license, the burden of replacing it with a REAL ID requiring an in-person visit was attributed to this rulemaking. The regulatory evaluation for the final rule employs the assumption that individuals who replace their lost or stolen legacy license will choose to obtain a REAL ID and pay the additional opportunity costs of an in-person visit to the DMV with the required source documents. After careful consideration, we believe that this assumption may be conservative based upon the revised requirements of the final rule. The enrollment periods of REAL ID have been designed to enable DMVs to enroll individuals with REAL IDs on their normal renewal cycles to the maximum extent possible. Individuals simply replacing a lost or stolen license are likely to want a replacement license as quickly as possible and delay the process of obtaining a REAL ID until their scheduled renewals. However, we maintain the original assumption in this economic analysis because we cannot estimate the different rate at which lost or stolen licenses will be replaced with REAL IDs. Therefore, we assume the rate to be 75% or the same as that for renewals.

The regulatory evaluation still assumes that States will move to central issuance because of the high cost of printing equipment for REAL ID cards. However, the final rule provides added flexibility and therefore States may not have to do this. We are not adjusting this regulatory evaluation to account for this due to uncertainties in States' behavior under the revised provisions of this final rule, and because there are remaining

requirements in this final rule that may still make central issuance the most efficient response.

9) The cost of security markings on REAL ID cards.

Based on discussions with State drivers' license card vendors, we have estimated the cost for a security marking for compliant cards to be $0.25 per card, and have included this cost estimate in the card production analysis later in this document.

The final rule also requires that if a State issues a license that is not in compliance with REAL ID, the State must by statute and regulation indicate on the document that it is not valid for official federal purposes. According to U.S. license vendors contacted by DHS[6], there is typically an upfront one time set up fee for the State, which may include license redesign, system reconfiguration, and other related costs. Based on our analysis of information received from vendors and States, DHS estimates that the added cost would be about $10,000 per State, or $.01 per document. The actual cost will vary depending on the State, vendor and any existing contractual agreement they may have concerning design changes. DHS believes that the added cost of no more than $0.01 per document will be indirectly incurred by those individuals who will be acquiring REAL ID's.

Summary of Major Differences Between the Final Rule and NPRM

Based upon the many comments received, the Final Rule incorporates major changes from the NPRM. The major changes impacting the economic analysis include:

1) Extension of Deadlines

[6] Based upon conversations between the REAL ID program office and U.S. license vendors, December, 2007.

In the NPRM, DHS proposed that States that would not be able to comply by May 11, 2008, should request an extension of the compliance date no later than February 10, 2008, and encouraged States to submit requests for extension as early as October 1, 2007. During the public comment period, DHS received numerous comments from States and Territories, State associations, and others, noting that almost all States would be unable to meet the May 2008 compliance deadline. Accordingly, to allow more time for States to implement the provisions of the rule in general and verification systems in particular, DHS is also providing in the final rule the opportunity for States to request extensions of the compliance date beyond the initial extension of December 31, 2009. To obtain a second extension, States must file a Material Compliance Checklist by October 11, 2009. This checklist will document State progress in meeting certain benchmarks toward full compliance with the requirements of this rule. States meeting the benchmarks shall be granted a second extension until no later than May 10, 2011. This would give States making significant progress additional time to meet all of the requirements of this rule.

2) Extended Enrollment Periods and Risk-Based Enrollment

The NPRM proposed that States determined by DHS to be in full compliance with the REAL ID Act and these implementing regulations by May 11, 2008, would have a five-year phase-in period – until May 11, 2013 – to replace all licenses intended for use for official purposes with REAL ID cards

During the public comment period, a number of States and State associations commented that States obtaining an initial extension of the compliance date until December 31, 2009, would still be required to enroll their existing driver population (estimated to be approximately 240 million) by May 11, 2013 – essentially halving the

phase-in period. Several commenters suggested that DHS employ a risk-based approach that would permit States and DMVs to focus first on perceived higher-risk individuals while deferring lower-risk individuals to a date beyond May 11, 2013.

DHS agrees with both these comments. Accordingly, in this final rule, DHS is extending the deadline for enforcing the provisions of the Act for all drivers' licenses and identification cards until no later than December 1, 2017, but requiring REAL ID-compliant drivers' licenses and identification cards for individuals 50 years of age or under (that is, individuals born on or after December 1, 1964) when used for official purposes beginning on December 1, 2014. This will effectively give States an eight-year enrollment period beginning in January 1, 2010 when Materially Compliant States can begin the enrollment process, thus avoiding an unnecessary operational burden on State DMVs from a crush of applicants on or before the original May 11, 2013 compliance date.

3) Physical Card Security

DHS has modified the proposed card security requirements in response to comments which stated that the requirements were too prescriptive and placed an undue burden on the States. Instead, DHS has proposed a performance-based approach that provides the flexibility for States to implement solutions using a well-designed balanced set of security features for cards that, when effectively combined, provide maximum resistance to counterfeiting, alteration, substitution, and the creation of fraudulent documents from legitimate documents.

4) Marking of Compliant REAL ID Documents

Based on an analysis of feedback from several commenters, DHS has determined that it would be in the best interest of the nation's security for States to place a security marking on drivers' licenses and identification cards that are issued in compliance with the REAL ID Act. Such a marking would facilitate the verification of the authenticity of such documents by Federal agencies requiring identification for official purposes.

5) Certification and Security Plan Documentation

Based on feedback from commenters, DHS has eased the reporting and documentation requirements placed upon States by circumscribing the scope of security plans and requiring submission of updated plans and certification packages on a rolling, triennial basis.

6) Address Change and Documentation Requirements

Based on numerous responses, DHS has removed the requirement that an address change must be accomplished through an in-person visit to the DMV. Additionally, there is no requirement in the final rule for States to issue a new card when notified of an address change. Moreover, DHS now allows States fuller discretion over the acceptance of address documents by removing specific requirements that documents used to demonstrate address of principal residence be issued "monthly" and "annually."

7) Financial Check

DHS agreed with comments that the financial history check would not be determinative. Therefore, DHS has eliminated the requirement for a financial history check from the final rule.

Costs and Benefits

This Regulatory Evaluation attempts to quantify or monetize the economic benefits of REAL ID. In spite of the difficulty, most everyone understands the benefits of secure and trusted identification. The final minimum standards seek to improve the security and trustworthiness of a key enabler of public and commercial life – State-issued drivers' licenses and identification cards. As detailed below, these standards will impose additional burdens on individuals, States, and even the Federal government. These costs, however, have been weighed against the quantifiable and nonquantifiable but no less real benefits to both public and commercial activities achieved by secure and trustworthy identification.

Economic Costs

Implementing the REAL ID Act will impact all 56 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 final rule over an eleven year period.

Figure 1: Estimated marginal economic cost of REAL ID final rule

Estimated Costs (11 years)	$ million 7% discounted	$ million 3% discounted	$ million (2006 dollars) undiscounted	% Total Undiscounted
Costs to States	**2,879**	**3,413**	**3,965**	**39.9%**
Customer Services	636	804	970	9.8%
Card production	690	822	953	9.6%
Data Systems & IT	1,171	1,352	1,529	15.4%
Security & Information Awareness	365	415	490	4.9%
Data Verification	5	7	8	0.1%
Certification process	11	13	16	0.2%
Costs to Individuals	**3,808**	**4,814**	**5,792**	**58.3%**
Opportunity Costs	3,429	4,327	5,215	52.5%
Application Preparation (125.8 million hours)	2,186	2,759	3,327	33.5%
Obtain Birth Certificate (20.1 million hours)	348	440	530	5.3%
Obtain Social Security Card (1.6 million hours)	31	37	44	0.4%
DMV visits (49.8 million hours)	864	1,091	1,315	13.2%
Expenditures: Obtain Birth Certificate	379	479	577	5.8%
Cost to Private Sector	**8**	**9**	**9**	**0.1%**
Costs to Federal Government	**128**	**150**	**171**	**1.7%**
Social Security card issuance	36	43	50	0.5%
Data Verification - SAVE	9	11	14	0.1%
Data Systems & IT	65	74	82	0.8%
Certification & training	17	21	25	0.3%
Total Costs	**6,853**	**8,406**	**9,939**	**100.0%**

Figure 1 shows the primary estimates calculated in both undiscounted 2006 dollars and discounted dollars at both the 3% and the 7% discounted rates. The total, undiscounted eleven-year cost of the final rule is $9.9 billion. Based on a total of 477.1 million issuances over the 11-years of the analysis, the average marginal cost per issuance for States is $8.30. Individuals will incur the largest share of the costs as shown in Figure ES–2. More than 58 percent of the costs (discounted or undiscounted) are associated

with preparing applications, obtaining necessary documents, or visiting motor vehicle offices.

The costs shown in Figure ES-2 show a substantial decrease in those reported in the NPRM. In particular, the costs for States are 27% of those estimated for the NPRM. This substantial decrease in costs can be attributed to a number of factors, including a revised assumption that only 75% of DL/ID holders will apply for a REAL ID as well as a less prescriptive, performance-based, and balanced approach to REAL ID implementation. As many commenters suggested, providing additional time for implementation and enrollment of DL/ID holders will allow States to accommodate the enrollment process without disrupting their normal renewal cycles, resulting in a decrease in total REAL ID issuances from 813 million to 477 million issuances. In addition, the undiscounted estimates for card production costs have decreased substantially from $5.8 billion in the NPRM to $953 million in the final rule based on the performance-based approach to card security standards recommended by numerous commenters.

DHS recognizes that many States have made significant progress in improving the integrity of their licenses. DHS also recognizes that the prescriptive technology standards included in the NPRM, compared to the final rule, provided relatively few additional security benefits at great cost to States. Moreover, the estimated opportunity costs to individuals have been reduced from $7.1 to $5.8 billion in undiscounted dollars primarily as a result of the changed assumption that only 75% of DL/ID holders will seek REAL IDs. Individuals will still have to obtain source documents and visit their DMVs under this analysis. Finally, the undiscounted costs to States for data systems and IT have actually increased from $1.4 billion in the NPRM to $1.5 billion in the final rule. This

slight increase reflects the critical role of information technology and verification systems in reducing identity theft and identity fraud in the issuance of DL/IDs.

The four largest cost areas, in descending order (in undiscounted dollars) are:

- opportunity costs to individuals ($5.2 billion),
- maintaining the necessary data and interconnectivity systems ($1.5 billion),
- customer service ($970 million), and
- card production and issuance ($953 million)

The largest impact category is the cost to individuals of obtaining source documents, preparing applications, and visiting DMVs. The magnitude of this category is driven largely by the fact that all applicants for a REAL ID will need to complete an application process similar to those of a first-time driver or a driver moving from one State to another.

The second largest impact category is the creation and maintenance of necessary data and interconnectivity systems. These systems will require substantial up-front effort to create but are likely to require smaller marginal increases in maintenance costs.

The third largest impact is customer service. While the extension of the enrollment period in the final rule will minimize marginal increases in the number or flow of transactions, the rule accounts for costs that increased transaction and wait times will produce. REAL ID should not substantially accelerate the rate of transactions, but the per transaction costs to States will increase.

The fourth largest impact is the production and issuance of the REAL IDs themselves. The final minimum standards are intended to make counterfeit production,

tampering and other fraud more difficult. While some State cards may already meet the standards of the final rule, many States may have to upgrade their cards and production processes in response to the rule. These upgrades will also require a substantial up-front effort followed by smaller marginal costs for subsequent years.

Estimated Benefits

The final REAL ID regulation will 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 REAL ID final rule seeks to improve the security and trustworthiness of a key enabler of public and commercial life – State-issued drivers' 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 gives 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 final rule.

DHS provides a "break-even" analysis based on the rule having an impact on the annual probability of the United States experiencing a 9/11 type attack in the 11 years following the issuance of the rule. It is exceedingly difficult to predict the probability and consequences of a hypothetical terrorist attack, DHS believes that those factors

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.

By making some generalized but conservative assumptions about the costs of attack consequences, DHS determined the reduction in probability of attack that REAL ID will need to bring about so that the expected cost of REAL ID equals its anticipated security benefits. DHS posed 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 United States 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.

DHS also developed an analysis based on the discounted cost of a single terrorist attack comparable to the 9/11 attacks on New York City and Washington, D.C. taking place sometime over an eleven-year span. The agency determined at what point the final rule would be cost-beneficial given the likelihood of an attack and the effectiveness of preventing the attack.

The final rule on REAL ID is likely to produce potential ancillary benefits as well. It will be more difficult to fraudulently obtain a legitimate license and more costly to create a false license, which could reduce identity theft, unqualified driving, and fraudulent activities facilitated by less secure drivers' 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 will bring about changes on the margin that will

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[7] (RFA), as amended, 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 rule will not have a significant economic impact on a substantial number of small entities.

The Department is implementing the regulations in order to enact the requirements outlined in the REAL ID Act.[8] This rule establishes minimum standards for the issuance of State-issued drivers' licenses and non-driver identification cards (DL/IDs). These minimum standards will:

- Enhance the security features of DL/IDs, rendering them more difficult to counterfeit, tamper with or cannibalize;
- Ensure that holders of unexpired REAL IDs are lawfully present in the United States;
- Enhance physical security of materials and production locations to reduce the likelihood of theft of materials and infiltration of DMVs by nefarious individuals;

[7] Regulatory Flexibility Act, Pub. L. No 96-354, 94 Stat. 1164 (codified at 5 U.S.C. § 601).
[8] *REAL ID Act of 2005*. Pub. L. 13, 109th Cong., 1st Sess. (May 11, 2005), 201, 202.

- Enhance identity source document requirements and verifications to reduce the number of DL/IDs issued by DMVs to persons committing identity fraud; and,
- Ensure that a REAL ID driver's license holder is licensed in only one State.

In short, these standards are designed to ensure that holders of unexpired REAL IDs are who they say they are and that they are lawfully present in the United States.

DHS did not receive any public comments on the Initial Regulatory Flexibility Analysis that was issued in support of the NPRM during the public comment period. All public comments are available for the public to view at the Federal Docket Management System: http://www.regulations.gov.

As part of this rulemaking effort, DHS has summarized and responded to all public comments relating to the Regulatory Evaluation issued with the NPRM. Comment summaries and responses are located in the preamble to the final rule, which is also available at http://www.regulations.gov and in the Federal Register.

The rule directly regulates States, which by definition are not small entities. The rule indirectly regulates entities that accept State-issued DL/IDs for official purposes. The rule defines those purposes as accessing Federal facilities, entering nuclear power plants and boarding federally regulated commercial aircraft. The entities that accept DL/IDs for those purposes include the Federal Government, operators of nuclear power plants and entities examining personal identity documents of people boarding federally regulated commercial aircraft. The rule does not require action from any of these three entities. However, these entities are likely to engage in some activity to ensure that they

comply with the Act. The remainder of this section estimates the number of small entities that are affected in this indirect way.

The Federal Government is not a small entity. Therefore, no small entities are affected by the prohibition on accepting State-issued DL/IDs that are not REAL IDs to access Federal facilities.

Nuclear power plants, though not directly regulated, may experience indirect impacts from this regulation. A nuclear power plant qualifies as a small entity 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."[9] With only three exceptions, every nuclear power plant in the United States produced more than 4 million megawatt hours in fiscal year 2005.[10] However, companies producing more than 12 million megawatt hours own each of those three plants.[11] None of the nuclear power plants qualifies as small businesses using the SBA definition. Therefore, no small entities are affected by the prohibition on accepting State-issued DL/IDs that are not REAL IDs to enter nuclear power plants.

Entities examining identity documents of people who are boarding federally regulated commercial aircraft will not be directly regulated by the rulemaking. However, they may experience indirect effects. Different types of entities examine personal

---

[9] 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 July 14, 2006.

[10] 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 July 14, 2006.

[11] 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.

identity documents of people boarding federally regulated commercial aircraft. Currently, this responsibility falls on the entity with whom passengers check their luggage, the entity examining boarding passes and IDs immediately in front of TSA screening checkpoints, and, when completed to fulfill federal requirements, the entities examining IDs directly before allowing passengers to board aircraft. The easiest group of entities to identify in this category is the airlines that enplane from and/or deplane into the sterile area of an airport.[12] The Small Business Administration considers companies operating either scheduled or non-scheduled chartered passenger air transportation to be small entities if they have fewer than 1,500 employees.[13] Using these criteria, DHS has identified 24 specific small entities that offer scheduled or non-scheduled air passenger transportation and that enplane from or deplane into an airport sterile area. Other federally regulated commercial aircraft include charter flights, air taxis, scenic air tours and other similar operations where the transportation of passengers for compensation comprises the majority of their revenues. Many of these entities would qualify as small entities under the SBA definition. SBA data show that, overall, 2,719 of the 2,877 firms engaged in air transportation (NAICS 481) had fewer than 500 employees in 2004.[14] Nearly all firms in the air transportation industry fall well below the 1,500-employee size standard to qualify as a small entity. (Note that the federal requirements may not require all of these firms to examine passenger identity documents prior to boarding.)

---

[12] "Sterile area" is defined in 49 CFR 1540.5 and generally means an area with access limited to persons who have undergone security screening by TSA. Therefore, only TSA-regulated airports have sterile areas.
[13] U.S. Small Business Administration. *Small Business Size Standards Matched to North American Industrial Classification System.* NAICS 481111 and 481211. Available at http://www.sba.gov/size/sizetable2002.html. Accessed July 14, 2006.
[14] U.S. Small Business Administration. *U.S. Data Classified by Employment Size of Firm: All industries, 2003-2004.* Available at http://www.sba.gov/advo/research/data.html. Accessed 4 Oct 2006.

DHS estimates that each employee accepting DL/IDs for official purposes will require two hours of training. This training will assist personnel in identifying the differences between REAL IDs and other State-issued DL/IDs. The training will also inform personnel about which States are or are not compliant during the enrollment period. In order to assess the cost of this training, 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. The next step to determine if firms' action will have a significant impact is to divide the summed products of wage rates and trained employees by firm revenue. Doing so yields the impact on the firm as a percent of their total receipts. However, data on how many employees firms will train do not exist on an industry level, much less at the firm level throughout the industry. Alternatively, a threshold analysis can determine at what point the revenue to trained employee ratio would constitute a one or three percent impact for a firm.

The Department has determined threshold levels that will cause an indirect impact equal to or less than one percent and equal to or greater than three percent of an entity's total revenue. If a firm's ratio is higher than the one percent threshold, the economic impact for that firm is not significant. If the ratio is lower than the three percent threshold, the economic impact will be larger than three percent of the firm's revenue. The threshold values are measured as the ratio of total revenue to the number of employees to be trained regarding REAL ID. If the amount of a firm's revenue per trained counter agent is more than $4,590, then the effect is less than one percent of total

revenue. If one percent requires revenue per agent of $4,590, then the three percent threshold revenue per agent lies at $1,530. If a firm's revenue per counter agent is less than $1,530, then the effect will be greater than three percent. The same approach can be applied to airport checkpoint staff yielding $4,501 at one percent and $1,500 at three percent. (See Figure **2**)

Figure 2: FRFA 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	$ 45.00

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

Applying the one percent threshold—the most stringent—to the 24 scheduled service firms specifically identified as small entities suggests that training employees regarding REAL ID will not impose a significant economic impact on a substantial number of small entities. Dividing a firm's total 2005 revenue by $4,590 yields an estimate of how many employees would need to be trained before the indirect impact reaches the one percent of total revenue threshold. Comparing that estimate to the number of employees at each firm in 2005 reveals that companies would need to train

anywhere from 6 to 56 times their total number of employees, including those who will not examine identification documents.[15]

The aggregated nature of industry-wide data does not allow for a firm-by firm analysis of the more than 2,719 small firms involved in air transportation. However, analysis of firms grouped by receipts in 2002 provides insight into the likelihood that entities will experience a significant indirect impact. Dividing receipts by the one percent threshold of $4,590 for each group estimates the number of employees that would result in a one percent impact on each group. The ratio of actual reported employees to threshold employees reveals that every group for which data is available would need to train multiple times more employees regarding REAL ID than they actually employ. The smallest ratio (largest impact) is for scheduled passenger air transportation (NAICS 48111) that earned less than $100,000, implying that they would need to train more than 11 times the number of people than they employed before the impact would reach one percent of their receipts.[16] The largest ratio (smallest impact in terms of percent of revenues) would fall on nonscheduled chartered passenger firms (NAICS 481211) earning more than $100 million. These firms would need to train more than 85 times the size of their workforce to reach the one percent impact threshold.

The combination of the firm specific analysis and the analysis of aggregated firms within receipt categories suggests that the indirect impact of training agents regarding REAL ID for the official purpose of boarding federally regulated commercial aircraft will not constitute a significant economic impact on a substantial number of small entities.

---

[15] Data from BTS (Form 41, Schedule P10); Duns and Bradstreet; Yahoo! Finance, and; Hoovers.com.
[16] Data from U.S. Small Business Administration. *U.S. All Industries by Receipt Size: 2002.* Available online at http://www.sba.gov/advo/research/data.html.Accessed 4 Oct 2006.

The above analyses show that it is unlikely that the prohibition on accepting State-issued DL/IDs unless they are REAL IDs will have a significant economic impact on a substantial number of small entities. Further, the only directly regulated entities are States, which by definition are not small entities. Therefore, the Department concludes that this rule will not have a significant economic impact on a substantial number of 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 non-driver identification cards. DHS has determined that this rule will 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 set forth in section 202(a)(1) of the REAL ID Act, the law is binding on Federal agencies—not on the States. Indeed, in the Conference Report, Congress specifically stated that the "application of the law is indirect, and hence States need not comply with the listed standards." Conf. Rep. at 177.

Moreover, 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 voluntary nature of the REAL ID Act, DHS assumes that States will willingly comply with the regulation to maintain the conveniences enjoyed by their residents when using their State-issued drivers' licenses and non-driver identity cards for official purposes, particularly as it pertains to domestic air travel. While, for the reasons set forth above, DHS believes that the REAL ID Act does not constitute an

unfunded mandate, DHS nevertheless believes that many States may find noncompliance an unattractive option.

Based on that knowledge, DHS has taken steps to comply with the requirements of UMRA. Specifically, DHS has analyzed the estimated cost to States and considered appropriate alternatives to, and benefits derived from, the final regulation. Moreover, DHS has solicited input from State and local governments in the preparation of this final rule.

C. Executive Order 13132, Federalism

Executive Order 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 this final rule is, without question, national in scope and significance. It is also one in which the States have significant equities.

While drivers' 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 individuals 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 drivers' 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 drivers' licenses; these documents were used to facilitate the terrorists' operations against the United States.[17]

1. DHS has Considered the Federalism Implications of the REAL ID Rule.

Section 3 of the Executive Order 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 Executive Order 13132 § 3(a) – (d) and submits the following:

a) Constitutional principles and maximizing the policymaking discretion of the States.

The rule is being promulgated in strict adherence to constitutional principles, and the limits of DHS's constitutional and statutory authority have been carefully considered. Congress, through the REAL ID Act, has mandated that Federal agencies refuse to accept for official purpose, State-issued drivers' licenses or identification cards unless DHS has determined that the issuing State is in compliance with the statutorily-mandated minimum standards for such identification documents. Notwithstanding the clear statutory mandate directing this rulemaking action, DHS has taken steps, in consultation with the States, to maximize policymaking discretion at the State level wherever possible.

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

For example, States may establish an exceptions process 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.

DHS also recognizes 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 final rule provides parameters for use by the States in determining which employees are "covered employees" and thus subject to the statutory background check requirements, but allows the individual States to determine which employees fall into categories deemed to be covered as defined under this final rule (e.g. DMV "employees or contractors who are involved in the manufacture or production of REAL ID drivers' licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card.").

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, and provides greater latitude in accepting alternatives or making exceptions based on State practices.

In other aspects of the proposed regulation DHS has prescribed baseline requirements while allowing States the discretion to impose more stringent standards, the greatest example of which is in the area of protecting personally identifiable information collected for REAL ID purposes. Most significantly, 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 final 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 incorporated into the regulation for States that do choose to participate. DHS believes that it has incorporated the maximum possible State discretion consistent with the purposes of the statute into this action.

c) Avoiding intrusive Federal oversight.

Consistent with Congress' vision for REAL ID (see § 202(a)(2) of the Act), States that choose to participate in the program will be responsible for monitoring their own compliance. Under the Act and the final 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 and DHS has adopted a certification process similar to that used by DOT in its regulations governing State administration of commercial drivers' licenses. States receiving adverse determinations will have the opportunity for an internal appeals process as well as judicial review.

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 rule. Accordingly, DHS has welcomed and encouraged State participation in this process and has sought, where possible, to draft this regulation in such a way as to maximize State discretion.

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.

2. The REAL ID Final Rule Complies with the Regulatory Provisions of Executive Order 13132.

Under § 6 of Executive Order 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 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 regulation.

a) The final 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 drivers' 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."[18] 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 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

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

cooperative Federalism" in which the Federal and State governments have acted voluntarily in tandem to achieve a common policy objective.[19]

b) DHS has engaged in extensive consultations with the States.

The statutory mandate and the lack of preemption both satisfy the requirements of Executive Order 13132. Nevertheless, in the spirit of Federalism, and consistent with § 205(a) of the REAL ID Act, DHS has engaged in extensive consultations with the States prior to issuing this final rule. As set forth earlier in this preamble of this 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, during the comment period, DHS hosted sessions that were available via webcast across the country to engage State Governors' chiefs of staff, homeland security directors in the States, and motor vehicles administrators, as well as a separate session with State legislators. DHS also convened the various stakeholder representatives that were identified as participants in the negotiated rulemaking group established under section 7212 of the Intelligence Reform and Terrorism Prevention Act. Further, DHS held a public meeting in Sacramento, California that was available nationwide via webcast and received comments from the public on a variety of topics, including consumer and personal impacts, privacy/ security, electronic verification systems, funding/implementation, and law enforcement.

d) DHS recognizes the burdens inherent in complying with the regulations.

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

[19] See id. at 167.

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 rule.

As indicated above, Executive Order 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 Executive Order 13132, section 6(b).

This 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 REAL ID regulation.

3. REAL ID and Federalism.

The issuance of drivers' 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 final rule, attempted to balance State prerogatives with the national interests at stake.

D. Environmental Impact Analysis

At the time of the proposed rule, DHS sought and received comment on the potential environmental impact of the physical standards and other proposed requirements under this rule. DHS carefully considered those comments in its evaluation of the potential environmental impacts of the rule. DHS concludes that the rule's potential impacts are minimal and this rule is a part of a category of actions that do not individually or cumulatively have a significant impact on the human environment and do not require a more extensive evaluation under the requirements of 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. DHS Categorical Exclusion A3 (Table 1 Management Directive 5100.1). Categorical Exclusion A3 applies to the promulgation of this rule, since it is of an administrative and procedural nature that does not force an immediate action but only lays the foundation for subsequent action. The categorical exclusion applies only to the promulgation of the REAL ID rule. Environmental impacts that may be associated with any follow-on DHS activity, such as approval of grant funding, must be reviewed if and when the subsequent program actions create the potential for environmental impact.

E. Energy Impact Analysis

The energy impact of this 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.

F. Executive Order 13175 (Tribal Consultation)

DHS has analyzed this final rule under Executive Order 13175 (entitled "Consultation and Coordination with Indian Tribal Governments", issued November 6, 2000). Executive Order 13175 states that no agency shall promulgate regulations that have tribal implications, that impose substantial direct compliance costs on Indian tribal governments, or that are not required by statute unless the agency first consults with tribal officials and prepares a tribal summary impact statement.

DHS has determined that this final rule will not have a substantial direct effect on one or more Indian tribes and will not impose substantial direct compliance costs on Indian tribal governments. This rule also does not seek to preempt any tribal laws. This final rule does not satisfy the tribal implications requirement in that it is a rule of general applicability that establishes minimum standards for State-issued drivers' licenses and identification cards that Federal agencies will accept for official purposes on or after May 11, 2008, a statutory mandate under the REAL ID Act of 2005. Therefore, tribal consultation and a tribal summary impact statement are not required.

List of Subjects in 6 CFR Part 37

Document security, drivers' licenses, identification cards, incorporation by reference, motor vehicle administrations, physical security.

THE AMENDMENTS

For the reasons set forth above, the Department of Homeland Security amends 6 CFR Chapter I by adding a new Part 37 as follows:

TITLE 6—HOMELAND SECURITY

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

PART 37—REAL ID DRIVERS' LICENSES AND IDENTIFICATION CARDS

Subpart A—General

Sec.

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

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

PART 37—REAL ID DRIVERS' LICENSES AND IDENTIFICATION CARDS

Subpart A--General

§ 37.01 Applicability.

(a) Subparts A through E of this rule apply to States and U.S. territories that choose to issue drivers' licenses and identification cards that can be accepted by Federal agencies for official purposes.

(b) Subpart F establishes certain standards for State-issued drivers' licenses and identification cards issued by States that participate in REAL ID, but that are not intended to be accepted by Federal agencies for official purpose under section 202(d)(11) of the REAL ID Act.

§ 37.03 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 Department of Motor Vehicles (DMV) or equivalent State office.

Certification means an assertion by the State to the Department of Homeland Security 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 in a registrant's State of birth.

Covered employees means Department of Motor Vehicles employees or contractors who are involved in the manufacture or production of REAL ID drivers' 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 validity of data contained in source documents presented under this regulation.

DHS means the U.S. Department of Homeland Security.

DMV means the Department of Motor Vehicles or any State Government entity that issues drivers' licenses and identification cards, or an office with equivalent function for issuing drivers' 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 drivers' licenses and identification cards issued by the State for official purposes.

Digital photograph means a digital image of the face of the holder of the driver's license or identification card.

Document authentication means determining 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, or State laws addressing domestic and dating violence.

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

Duplicate means a driver's license or identification card issued subsequent to the original document that bears the same information and expiration date as the original document and that is reissued at the request of the holder when the original is lost, stolen, or damaged and there has been no material change in information since prior issuance.

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 compliance means that the Secretary or his designate(s) has determined that a State has met all the requirements of Subparts A through E.

Full legal name means an individual's first name, middle name(s), and last name or surname, without use of initials or nicknames

IAFIS means the Integrated Automated Fingerprint Identification System, a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (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 or State office with equivalent function which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.

INS means the former-Immigration and Naturalization Service of the U.S. Department of Justice.

Lawful status: A person in lawful status is a citizen or national of the United States; or an alien (i) lawfully admitted for permanent or temporary residence in the United States; (ii) with conditional permanent resident status in the United States; (iii) who has an approved application for asylum in the United States or has entered into the United States in refugee status; (iv) who has a valid nonimmigrant status in the United States; (v) who has a pending application for asylum in the United States; (vi) who has a pending or approved application for temporary protected status (TPS) in the United States; (vii) who has approved deferred action status; or (viii) who has a pending application for lawful permanent residence (LPR) or conditional permanent resident status. This definition does not affect other definitions or requirements that may be contained in the Immigration and Nationality Act or other laws.

Material Change means any change to the personally identifiable information of an individual as defined under this Rule. Notwithstanding the definition of personally identifiable information below, a change of address of principal residence does not constitute a material change.

Material Compliance means a determination by DHS that a State has met the benchmarks contained in the Material Compliance Checklist.

NCIC means the National Crime Information Center, a computerized index of criminal justice information maintained by the Federal Bureau of Investigation (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 U.S. 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 U.S. Department of State.

Personally Identifiable Information means any information which can be used to distinguish or trace an individual's identity, such as their name; driver's license or identification card number; social security number; biometric record, including a digital photograph or signature; alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as a date and place of birth or address, whether it is stored in a database, on a driver's license or identification card, or in the machine readable technology on a license or identification card.

Principal residence means the location where a person currently resides (i.e., presently resides even if at a temporary address) in conformance with the residency requirements of the State issuing the driver's license or identification card, if such requirements exist.

REAL ID Driver's License or Identification Card means a driver's license or identification card that has been issued by a State that has been certified by DHS to be in compliance with the requirements of the REAL ID Act and which meets the standards of subparts A through D of this Part, including temporary or limited-term drivers' licenses or identification cards issued under § 37.21.

Reissued card means a card that a State DMV issues to replace a card that has been lost, stolen or damaged, or to replace a card that includes outdated information. A card may not be reissued remotely when there is a material change to the personally identifiable information as defined by the Rule.

Renewed card means a driver's license or identification card that a State DMV issues to replace a renewable driver's license or identification card.

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, or State laws addressing sexual assault and stalking.

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.

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 or other categories of persons.

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.

Verify means procedures to ensure that: (1) the source document is genuine and has not been altered (i.e., "document authentication"); and (2) the identity data contained on the document is valid ("data verification").

§ 37.05 Validity periods and deadlines for REAL ID drivers' licenses and identification cards.

(a) Drivers' licenses and identification cards issued under this Part, that are not temporary or limited-term drivers' licenses and identification cards, are valid for a period not to exceed eight years. A card may be valid for a shorter period based on other State or Federal requirements.

(b) On or after December 1, 2014, Federal agencies shall not accept a driver's license or identification card for official purposes from individuals born after December 1, 1964, unless such license or card is a REAL ID-compliant driver's license or

identification card issued by a State that has been determined by DHS to be in full compliance as defined under this subpart.

(c) On or after December 1, 2017, Federal agencies shall not accept a driver's license or identification card for official purposes from any individual unless such license or card is a REAL ID-compliant driver's license or identification card issued by a State that has been determined by DHS to be in full compliance as defined under this subpart.

(d) Federal agencies cannot accept for official purpose drivers' licenses and identification cards issued under § 37.71 of this rule.

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

§ 37.11 Application and documents the applicant must provide.

(a) The State must subject each person applying for a REAL ID driver's license or identification card to a mandatory facial image capture, and shall maintain photographs of individuals even if no card is issued. The photographs must be stored in a format in accordance with § 37.31 as follows:

(1) If no card is issued, for a minimum period of five years.

(2) If a card is issued, for a period of at least two years beyond the expiration date of the card.

(b) Declaration. Each applicant must sign a declaration under penalty of perjury that the information presented on the application is true and correct, and the State must retain this declaration. An applicant must sign a new declaration when presenting new source documents to the DMV on subsequent visits.

(c) Identity.

(1) To establish identity, the applicant must present at least one of the following source documents:

(i) Valid, unexpired U.S. passport.

(ii) Certified copy of a birth certificate filed with a State Office of Vital Statistics or equivalent agency in the individual's State of birth.

(iii) Consular Report of Birth Abroad (CRBA) issued by the U.S. Department of State, Form FS-240, DS-1350 or FS-545.

(iv) Valid, unexpired Permanent Resident Card (Form I-551) issued by DHS or INS.

(v) 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 accompanied by the approved I-94 form documenting the applicant's most recent admittance into the United States.

(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, issued by DHS.

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

(x) Such other documents as DHS may designate by notice published in the Federal Register.

(2) Where a State permits an applicant to establish a name other than the name that appears on a source document (for example, through marriage, adoption, court order, or other mechanism permitted by State law or regulation), the State shall require evidence

of the name change through the presentation of documents issued by a court, governmental body or other entity as determined by the State. The State shall maintain copies of the documentation presented pursuant to § 37.31, and maintain a record of both the recorded name and the name on the source documents in a manner to be determined by the State and in conformity with § 37.31.

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

(e) Social security number (SSN).

(1) Except as provided in paragraph (3) below, individuals presenting the identity documents listed in § 37.11(c)(1) and (2) must present his or her Social Security Administration account number card; or, if a Social Security Administration account card is not available, the person may present any of the following documents bearing the applicant's SSN (i) a W-2 form, (ii) a SSA-1099 form, (iii) a non-SSA-1099 form, or (iv) a pay stub with the applicant's name and SSN on it;

(2) The State DMV must verify the SSN pursuant to § 37.13(b)(2) of this subpart.

(3) Individuals presenting the identity document listed in § 37.11(c)(1)(vi) must present an SSN or demonstrate non-work authorized 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. A street address is required except as provided in § 37.17(f) of this Part.

(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.

(1) If the applicant presents one of the documents listed under paragraphs (c)(1)(i), (c)(1)(ii), (c)(1)(iii), (c)(1)(iv), (c)(1)(vii) or (c)(1)(viii), the issuing State's verification of the applicant's identity in the manner prescribed in § 37.13 will also provide satisfactory evidence of lawful status.

(2) If the applicant presents one of the identity documents listed under paragraphs (c)(1)(v) or (c)(1)(vi), or (c)(1)(ix), the issuing State's verification of the identity document(s) does not provide satisfactory evidence of lawful status. The applicant must also present a second document from § 37.11(g)(1) or documentation issued by DHS or other Federal agencies demonstrating lawful status as determined by USCIS. All documents shall be verified in the manner prescribed in § 37.13.

(h) Exceptions Process. A State DMV may choose to establish a written, defined exceptions process for persons who, for reasons beyond their control, are unable to present all necessary documents and must rely on alternate documents to establish identity or date of birth. Alternative documents to demonstrate lawful status will only be allowed to demonstrate U.S. citizenship.

(1) Each State establishing an exceptions process must make reasonable efforts to establish the authenticity of alternate documents each time they are presented and indicate that an exceptions process was used in the applicant's record.

(2) The State shall retain copies or images of the alternate documents accepted pursuant to § 37.31 of this part.

(3) The State shall conduct a review of the use of the exceptions process, and pursuant to Subpart E, prepare and submit a report with a copy of the exceptions process as part of the certification documentation detailed in §37.55.

(i) States are not required to comply with these requirements when issuing REAL ID drivers' licenses or identification cards in support of Federal, State, or local criminal justice agencies or other 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. Drivers' 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.

§ 37.13 Document verification requirements.

(a) States shall make reasonable efforts to ensure that the applicant does not have more than one driver's license or identification card already issued by that State under a different identity. In States where an individual is permitted to hold both a driver's license and identification card, the State shall ensure that the individual has not been issued identification documents in multiple or different names.

(1) States shall also comply with the provisions of § 37.29 before issuing a driver's license or identification card.

(b) States must verify the documents and information required under § 37.11 with the issuer of the document. States shall use systems for electronic validation of document and identity data as they become available or use alternative methods approved by DHS.

(1) States shall verify any document described in § 37.11(c) or (g) and issued by DHS (including, but not limited to, the I-94 form described in § 37.11(c)(vi)) through the Systematic Alien Verification for Entitlements (SAVE) system or alternate methods approved by DHS, except that if two DHS-issued documents are presented, a SAVE verification of one document that confirms lawful status does not need to be repeated for the second document. In the event of a non-match, the DMV must not issue a REAL ID driver's license or identification card to an applicant, and must refer the individual to U.S. Citizenship and Immigration Services for resolution.

(2) States must verify SSNs with the Social Security Administration (SSA) or through another method approved by DHS. In the event of a non-match with SSA, a State may use existing procedures to resolve non-matches. If the State is unable to resolve the non-match, and the use of an exceptions process is not warranted in the situation, the DMV must not issue a REAL ID driver's license or identification card to an applicant until the information verifies with SSA.

(3) States must verify birth certificates presented by applicants. States should use the Electronic Verification of Vital Events (EVVE) system or other electronic systems whenever the records are available. If the document does not appear authentic upon inspection or the data does not match and the use of an exceptions process is not warranted in the situation, the State must not issue a REAL ID driver's license or

identification card to the applicant until the information verifies, and should refer the individual to the issuing office for resolution.

(4) States shall verify documents issued by the Department of State with the Department of State or through methods approved by DHS.

(5) States must verify REAL ID drivers' licenses and identification cards with the State of issuance.

(6) Nothing in this section precludes a State from issuing an interim license or a license issued under § 37.71 that will not be accepted for official purposes to allow the individual to resolve any non-match.

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

(a) General. States must include document security features on REAL ID drivers' licenses and identification cards designed to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards in accordance with this section.

(1) These features must not be capable of being reproduced using technologies that are commonly used and made available to the general public.

(2) The proposed card solution must contain a well-designed, balanced set of features that are effectively combined and 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 drivers' licenses and identification cards must contain at least three levels of integrated security features that provide the maximum resistance to persons' efforts to--

(1) Counterfeit, alter, simulate, or reproduce a genuine document;

(2) Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder;

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

(4) Create a fraudulent document using components from legitimate drivers' 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) Document security and integrity. States must conduct a review of their card design and submit a report to DHS with their certification that indicates the ability of the design to resist compromise and document fraud attempts. The report required by this paragraph is SSI and must be handled and protected in accordance with 49 CFR Part 1520. Reports must be updated and submitted to DHS whenever a security feature is modified, added, or deleted.

(1) After reviewing the report, DHS may require a State to provide DHS with examination results from a recognized independent laboratory experienced with adversarial analysis of identification documents concerning one or more areas relating to the card's security.

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

To be accepted by a Federal agency for official purposes, REAL ID drivers' licenses and identification cards must include on the front of the card (unless otherwise specified below) the following information:

(a) Full legal name. Except as permitted in § 37.11(c)(2), the name on the face of the license or card must be the same as the name on the source document presented by the applicant to establish identity.

(1) Where the individual has only one name, that name should be entered in the last name or family name field, and the first and middle name fields should be left blank. Place holders such as NFN, NMN, and NA should not be used.

(b) Date of birth.

(c) Gender, as determined by the State.

(d) Unique Driver's license or identification card number. This cannot be the individual's SSN, and must be unique across driver's license or identification cards within the State.

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

(1) States shall follow the current ICAO standards, specifically ISO/IEC 19794-5—Information technology—Biometric Data Interchange Formats—Part 5: Face Image Data. 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 at www.mrtd.icao.int. One may inspect a copy at the Office of the Federal

Register, 800 N. Capitol Street, N.W., Suite 700, Washington D.C. These standards include:

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

(ii) The face from crown to the base of the chin, and from ear-to-ear, shall be clearly visible and free of shadows.

(iii) 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 and must not take any action to obstruct a photograph of their facial features.

(iv) Where possible, 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.

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

(2) Photographs may be in black and white or color.

(f) Address of principal residence, except an alternative address may be displayed for:

(1) individuals for whom a State law, regulation, or DMV procedure permits display of an alternative address, or

(2) individuals who satisfy any of the following:

(i) If the individual is enrolled in a State address confidentiality program which allows victims of domestic violence, dating violence, sexual assault, stalking, or a severe form of trafficking, to keep, obtain, and use alternative addresses; and provides that the addresses of such persons must be kept confidential, or other similar program;

(ii) If the individual's address is entitled to be suppressed under State or Federal law or suppressed by a court order including an administrative order issued by a State or Federal court; or

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

(3) In areas where a number and street name has not been assigned for U.S. mail delivery, an address convention used by the U.S. Postal Service is acceptable.

(g) 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 www.aamva.org, or by contacting AAMVA at 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203, tel. (703) 522-4200. One may inspect a copy at the Office of the Federal Register, 800 N. Capitol Street, N.W., Suite 700, Washington D.C.

The State shall establish alternative procedures for individuals unable to sign their name.

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

(i) Machine-readable technology on the back of the card, pursuant to § 37.19 of this subpart.

(j) Date of transaction.

(k) Expiration date.

(l) State or territory of issuance.

(m) 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 Latin alpha-numeric characters. The name must contain a field of no less than a total of 39 characters, and longer names shall 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, N.W., Suite 700, Washington D.C.

(n) The card shall bear a DHS-approved security marking on each driver's license or identification card that is issued reflecting the card's level of compliance as set forth in § 37.51 of this Rule.

§ 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 the PDF417 2D bar code standard, with the following defined minimum data elements:

(a) Expiration date.

(b) Full legal name, unless the State permits an applicant to establish a name other than the name that appears on a source document, pursuant to § 37.11(c)(2).

(c) Date of transaction.

(d) Date of birth.

(e) Gender.

(f) Address as listed on the card pursuant to § 37.17(f).

(g) Unique driver's license or identification card number.

(h) Card design 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.

(j) State or territory of issuance.

§ 37.21 Temporary or limited-term drivers' licenses and identification cards.

States may only issue a temporary or limited-term REAL ID 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 or limited-term driver's license or identification card to a person, valid documentary evidence, verifiable through SAVE or other DHS-approved means, that the person has lawful status in the United States.

(b) States shall not issue a temporary or limited-term 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; and

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

(c) States shall renew a temporary or limited-term driver's license or identification card pursuant to this section and § 37.25(b)(2), only if:

(1) the individual presents valid documentary evidence that the status by which the applicant qualified for the temporary or limited-term driver's license or identification card is still in effect, or

(2) the individual presents valid documentary evidence that he or she continues to qualify for lawful status under paragraph (a) of this section.

(d) States must verify the information presented to establish lawful status through SAVE, or another method approved by DHS.

(e) Temporary or limited-term drivers' licenses and identification cards must clearly indicate on the face of the license and in the machine readable zone that the license or card is a temporary or limited-term driver's license or identification card.

§ 37.23 Reissued REAL ID drivers' licenses and identification cards.

(a) 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 reissued, to ensure that the individual receiving the reissued REAL ID driver's license or identification card is the same individual to whom the driver's license or identification card was originally issued.

(b) Remote/Non-in-person reissuance. Except as provided in (c) of this section a State may conduct a non-in-person (remote) reissuance if State procedures permit the reissuance to be conducted remotely. Except for the reissuance of duplicate drivers'

licenses and identification cards as defined in this rule, the State must reverify pursuant to § 37.13, the applicant's SSN and lawful status prior to reissuing the driver's license or identification card.

(c) In-person reissuance. The State may not remotely reissue a driver's license or identification card where there has been a material change in any personally identifiable information since prior issuance. All material changes must be established through an applicant's presentation of an original source document as provided in this subpart, and must be verified as specified in § 37.13.

§ 37.25 Renewal of REAL ID drivers' licenses and identification cards.

(a) In-person renewals. States must require holders of REAL ID drivers' licenses and identification cards to renew their drivers' licenses and identification cards with the State DMV in person, no less frequently than every sixteen years.

(1) The State DMV shall take an updated photograph of the applicant, no less frequently than every sixteen years.

(2) The State must reverify the renewal applicant's SSN and lawful status through SSOLV and SAVE, respectively (or other DHS-approved means) as applicable prior to renewing the driver's license or identification card. The State must also verify electronically information that it was not able to verify at a previous issuance or renewal if the systems or processes exist to do so.

(3) Holders of temporary or limited-term REAL ID drivers' licenses and identification cards must present evidence of continued lawful status via SAVE or other method approved by DHS when renewing their driver's license or identification card.

(b) Remote/Non-in-person renewal. Except as provided in (b)(2) a State may conduct a non-in-person (remote) renewal if State procedures permit the renewal to be conducted remotely.

(1) The State must reverify the applicant's SSN and lawful status pursuant to § 37.13 prior to renewing the driver's license or identification card.

(2) The State may not remotely renew a REAL ID driver's license or identification card where there has been a material change in any personally identifiable information since prior issuance. All material changes must be established through the applicant's presentation of an original source document as provided in Subpart B, and must be verified as specified in § 37.13.

§ 37.27 Drivers' licenses and identification cards issued during the age-based enrollment period

Drivers' licenses and identification cards issued to individuals prior to a DHS determination that the State is materially compliant may be renewed or reissued pursuant to current State practices, and will be accepted for official purposes until the validity dates described in § 37.05. Effective December 1, 2014, Federal agencies will only accept REAL ID cards for official purpose from individuals under 50 as of December 1, 2014. Individuals age 50 or older on December 1, 2014, must obtain and present REAL ID cards for official purposes by December 1, 2017.

§ 37.29 Prohibition Against Holding More than One REAL ID Card or More than One Driver's License.

(a) An individual may hold only one REAL ID card. An individual cannot hold a REAL ID driver's license and a REAL ID identification card simultaneously. Nothing

shall preclude an individual from holding a REAL ID card and a non-REAL ID card unless prohibited by his or her State.

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

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

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

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

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

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

Subpart C--Other Requirements

§ 37.31 Source document retention.

(a) States must retain copies of the application, declaration and source documents presented under § 37.11 of this Part, including documents used to establish all names recorded by the DMV under § 37.11(c)(2). States shall take measures to protect any

personally identifiable information collected pursuant to the REAL ID Act as described in their security plan under § 37.41(b)(2).

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

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

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

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

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

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

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

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

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

§ 37.33 DMV databases.

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

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

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

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

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

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

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

§ 37.41 Security plan.

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

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

(1) Physical security for the following:

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

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

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

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

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

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

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

(4) Access control, including the following:

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

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

(iii) Controlled access systems.

(5) Periodic training requirements in--

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

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

(6) Emergency/incident response plan;

(7) Internal audit controls;

(8) An affirmation that the State possesses both the authority and the means to produce, revise, expunge, and protect the confidentiality of REAL ID drivers' licenses or identification cards issued in support of Federal, State, or local criminal justice agencies or similar programs that require special licensing or identification to safeguard persons or support their official duties. These procedures must be designed in coordination with the key requesting authorities to ensure that the procedures are effective and to prevent conflicting or inconsistent requests. In order to safeguard the identities of individuals,

these procedures should not be discussed in the plan and States should make every effort to prevent disclosure to those without a need to know about either this confidential procedure or any substantive information that may compromise the confidentiality of these operations. The appropriate law enforcement official and United States Attorney should be notified of any action seeking information that could compromise Federal law enforcement interests.

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

§ 37.43 Physical security of DMV production facilities.

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

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

§ 37.45 Background checks for covered employees.

(a) Scope. States are required to subject persons who are involved in the manufacture or production of REAL ID drivers' licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card, or current employees who will be assigned to such positions ("covered employees" or "covered positions"), to a background check. The background check must include, at a minimum, the validation of references from prior employment, a name-based and fingerprint-based criminal history records check, and employment

eligibility verification otherwise required by law. States shall describe their background check process as part of their security plan, in accordance with § 37.41(b)(4)(ii). This section also applies to contractors utilized in covered positions.

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

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

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

(ii) Interim disqualifying criminal offenses. The criminal offenses referenced in 49 CFR 1572.103(b) are disqualifying if the covered employee 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 employment in the covered position; or the covered employee was released from incarceration for the crime within the five years preceding the date of employment in the covered position.

(iii) Under want or warrant. A covered employee 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) or (b)(1)(iv) of this section under circumstances determined by the State. These procedures can cover circumstances where the covered employee has been arrested, but no final disposition of the matter has been reached.

(2) Employment eligibility status verification. The State shall ensure it is fully in compliance with the requirements of section 274A of the Immigration and Nationality Act (8 U.S.C. 1324a) and its implementing regulations (8 C.F.R. Part 274A) with respect to each covered employee. The State is encouraged to participate in the USCIS E-Verify program (or any successor program) for employment eligibility verification.

(3) Reference check. Reference checks from prior employers are not required if the individual has been employed by the DMV for at least two consecutive years since May 11, 2006.

(4) Disqualification. If results of the State's CHRC reveal a permanent disqualifying criminal offense under paragraph (b)(1)(i) or an interim disqualifying criminal offense under paragraph (b)(1)(ii), the covered employee may not be employed in a position described in paragraph (a) of this section. An employee whose employment eligibility has not been verified as required by section 274A of the Immigration and

Nationality Act (8 U.S.C. 1324a) and its implementing regulations (8 C.F.R. Part 274A) may not be employed in any position.

(c) Appeal. If a State determines that the results from the CHRC do not meet the standards of such check the State must so inform the employee of the determination to allow the individual an opportunity to appeal to the State or Federal government, as applicable.

(d) Background checks substantially similar to the requirements of this section that were conducted on existing employees on or after May 11, 2006 need not be re-conducted.

Subpart E—Procedures for Determining State Compliance

§ 37.51 Compliance—general requirements.

(a) Full compliance. To be in full compliance with the REAL ID Act of 2005, 49 U.S.C. 30301 note, States must meet the standards of subparts A through D or have a REAL ID program that DHS has determined to be comparable to the standards of subparts A through D. States certifying compliance with the REAL ID Act must follow the certification requirements described in § 37.55. States must be fully compliant with Subparts A through D on or before May 11, 2011. States must file the documentation required under §37.55 at least 90 days prior to the effective date of full compliance.

(b) Material compliance. States must be in material compliance by January 1, 2010 to receive an additional extension until no later than May 10, 2011 as described in § 37.63. Benchmarks for material compliance are detailed in the Material Compliance Checklist found in Appendix A to this rule.

§ 37.55 State certification documentation.

(a) States seeking DHS's determination that its program for issuing REAL ID drivers' licenses and identification cards is meeting the requirements of this Part (full compliance), must provide DHS with the following documents:

(1) A certification by the highest level Executive official in the State overseeing the DMV reading as follows:

> "I, [name and title(name of certifying official), (position title) of the State (Commonwealth))] of ___, do hereby certify that the State (Commonwealth) has implemented a program for issuing drivers' 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."

(2) 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.

(3) A description of the State's exceptions process under § 37.11(h), and the State's waiver processes under § 37.45(b)(1)(v).

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

(b) After DHS's final compliance determination, States shall recertify compliance with this Part every three years on a rolling basis as determined by DHS.

§ 37.59 DHS reviews of State compliance.

State REAL ID programs will be subject to DHS review to determine whether 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 at any time. In addition, the State must:

(1) Provide any reasonable information pertinent to determining compliance with this part as requested by DHS;

(2) Permit DHS to conduct inspections of any and all sites associated with the enrollment of applicants and the production, manufacture, personalization and issuance of drivers' licenses or identification cards; and

(3) Allow DHS to conduct interviews of the State's employees and contractors who are involved in the application and verification process, or the manufacture and production of drivers' licenses or identification cards. DHS shall provide written notice to the State in advance of an inspection visit.

(b) Preliminary DHS determination. DHS shall review forms, conduct audits of States as necessary, and make a preliminary determination on whether the State has satisfied the requirements of this Part within 45 days of receipt of the Material Compliance Checklist or State certification documentation of full compliance pursuant to § 37.55.

(1) If DHS determines that the State meets the benchmarks of the Material Compliance Checklist, DHS may grant the State an additional extension until no later than May 10, 2011.

(2) If DHS determines that the State meets the full requirements of Subparts A through E, the Secretary shall make a final determination that the State is in compliance with the REAL ID Act.

(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 any deficiencies cited in the

preliminary determination or, alternatively, detail why the DHS preliminary determination is incorrect. Upon request by the State, an informal conference will be scheduled during this time.

(d) Final DHS determination. DHS will notify States of its final determination of State compliance with this Part, within 45 days of receipt of a State reply.

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

(b) The Secretary will determine that a State is not in compliance with this Part when it--

(1) Fails to submit a timely certification or request an extension as prescribed in this subpart; or

(2) Does not meet one or more of the standards of this Part, as established in a determination by DHS under § 37.59.

§ 37.63 Extension of deadline.

(a) A State may request an initial extension by filing a request with the Secretary no later than [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER.]. 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.

(i) DHS shall notify a State of its acceptance of the State's request for initial extension within 45 days of receipt.

(b) States granted an initial extension may file a request for an additional extension until no later than May 10, 2011, by submitting a Material Compliance Checklist demonstrating material compliance, per §37.51(b) with certain elements of Subparts A through E as defined by DHS. Such additional extension request must be filed by October 11, 2009.

(i) DHS shall notify a State whether an additional extension has been granted within 45 days of receipt of the request and documents described above.

(c) Subsequent extensions, if any, will be at the discretion of the Secretary.

§ 37.65 Effect of failure to comply with this Part.

(a) Any driver's license or identification card issued by a State that DHS determines is not in compliance with this Part is not acceptable as identification by Federal agencies for official purposes.

(b) Drivers' licenses and identification cards issued by a State that has obtained an extension of the compliance date from DHS per § 37.51 are acceptable for official purposes until the end of the applicable enrollment period under § 37.05; or the State subsequently is found by DHS under this Subpart to not be in compliance.

(c) Drivers' licenses and identification cards issued by a State that has been determined by DHS to be in material compliance and that are marked to identify that the licenses and cards are materially compliant will continue to be accepted by Federal agencies after the expiration of the enrollment period under § 37.05, until the expiration date on the face of the document.

Subpart F –Drivers' Licenses and Identification Cards Issued Under Section 202(d)(11) of the REAL ID Act

§ 37.71 Drivers' licenses and identification cards issued under section 202(d)(11) of the REAL ID Act.

(a) Except as authorized in § 37.27, States that DHS determines are compliant with the REAL ID Act that choose to also issue drivers' licenses and identification cards that are not acceptable by Federal agencies for official purposes must ensure that such drivers' licenses and identification cards--

(1) Clearly state on their face and in the machine readable zone that the card is not acceptable for official purposes; and

(2) Have a unique design or color indicator that clearly distinguishes them from drivers' licenses and identification cards that meet the standards of this Part.

(b) DHS reserves the right to approve such designations, as necessary, during certification of compliance.

* * * * *

Issued in Washington, DC, on January 10, 2008.

Michael Chertoff

Secretary

APPENDIX A: MATERIAL COMPLIANCE CHECKLIST

Material Compliance Checklist

#	Section	Does the State	Yes, is met	No, will meet by [date]	Special Instructions
1	§ 37.11(a)	Subject each applicant to a mandatory facial image capture and retain such image even if a driver license (DL) or identification card (ID) is not issued			
2	§ 37.11(b)	Have each applicant sign a declaration under penalty of perjury that the information presented is true and correct, and the State must retain this declaration			
3	§ 37.11(c) (1)	Require an individual to present at least one of the source documents listed in subsections (i) through (x) when establishing identity			
4	§ 37.11(d)-(g)	Require documentation of: • Date of birth • Social Security Number • Address of principal residence • Evidence of lawful status			
5	§ 37.11(h)	Have a documented exceptions process that meets the requirements established in 37.11(h)(1)-(3) (if States choose to have such a process)			
6	§ 37.13(a)	Make reasonable efforts to ensure that the applicant does not have more than one DL or ID already issued by that State under a different identity			Describe measures taken
7	§ 37.13(b)(1)	Verify lawful status through SAVE or another method approved by DHS			If not through SAVE, describe method
8	§ 37.13(b)(2)	Verify Social Security account numbers with the Social Security Administration or another method approved by DHS			If not through SSOLV, describe method
9	§ 37.15(b)	Issue DL and IDs that contain Level 1, 2 and 3 integrated security features			

10	§ 37.17(a)-(l)	Surface (front and back) of cards include the following printed information in Latin alpha-numeric characters: • Full legal name • Date of birth • Gender • Unique DL/ID number • Full facial digital photograph • Address of principal residence [with exceptions] • Signature [with exceptions] • Date of transaction • Expiration date • State or territory of issuance
11	§ 37.17 (n)	Commit to mark materially compliant DL and IDs with a DHS-approved security marking.
12	§ 37.21	Issue temporary or limited-term licenses to all individuals with temporary lawful status and tie license validity to the end of lawful status
13	§ 37.41	Have a documented security plan for DMV operations in accordance with the requirements set forth in § 37.41
14	§ 37.41(b)(2)	Have protections in place to ensure the security of personally identifiable information
15	§ 37.41(b)(5) (i)-(ii)	Require all employees handling source documents or issuing DLs or IDs to attend and complete the AAMVA approved (or equivalent) fraudulent document recognition training and security awareness training
16	§ 37.45	Conduct name-based and fingerprint-based criminal history and employment eligibility checks on all employees in covered positions or an alternative procedure approved by DHS
17	§ 37.51 (b)(1)	Commit to be in material compliance with Subparts A through D no later than January 1, 2010 or within 90 days of submission of this document, whichever date is earlier
18	§ 37.71 (b)(1)	Clearly state on the face of non-compliant DLs or IDs that the card is not acceptable for official purposes, except for licenses renewed or reissued under § 37.27