

Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

Real ID Regulations ...Finally *Updated February 12, 2008*

Brief 1

Deadlines, Definition of Official Purpose, Reenrollment, State Certification and Reporting, State Exceptions Process, and Funds

On January 11, 2008, the Department of Homeland Security (DHS) issued the long awaited final regulations on Real ID Act implementation, a mere **120 days before the May 11, 2008 deadline**. The regulations were printed in the *Federal Register* on January 29, 2008. The final regulations incorporate a number of recommendations made to DHS by NCSL, governors and motor vehicle administrators. However, DHS still estimates the cost of implementation to the states at \$3.99 billion.

Over the next week, NCSL will publish a series of briefs summarizing different sections of the regulations. In addition, this will include a comparison of the requirements to the recommendations included in the September 2006 report— *The Real ID: National Impact Analysis*—issued by NCSL, governors and motor vehicle administrators. Brief 2 will focus on Physical Security of DMV Facilities and Databases, and Employee and Applicant Background Checks.

A copy of the final regulations, the September 2006 report, and other resources on Real ID are available at: <http://www.ncsl.org/realid>

State Deadlines

In order for a state's driver's license (DL) or identification card (ID) to be accepted for federal purposes, a state must certify to DHS that the state is compliant with the requirements of the Real ID on or before May 11, 2008. Initially, state certification may take two forms:

- A state may certify that it fully complies with the requirements of the Real ID; **OR**
- A state may request an initial extension **by March 31, 2008**. DHS will notify states of the initial extension within 45 days or receipt of the state's request. The initial extension would expire on December 31, 2009.

States may request an additional extension until May 10, 2011, by submitting a Material Compliance Checklist (see *State Certification and Reporting* below), which requires states to indicate their level of compliance with the Real ID. States must file for the additional extension by October 11, 2009.

Additional extensions may be granted at the discretion of Secretary of Homeland.

A state-issued DL and ID will be accepted for federal purposes if a state has received an extension or the state is deemed fully compliant with the requirements of the Real ID.

Official Purpose

As recommended by NCSL, governors and motor vehicle administrators, the final regulations limit the "official purpose" of the Real ID to the uses expressly stated in the Act: accessing federal facilities, boarding commercial aircraft and entering nuclear power plants.

Reenrollment

A state-issued DL and ID must meet the requirements of the Real ID:

- By December 1, 2014 for individuals born after December 1, 1964; AND
- By December 1, 2017 for individuals born before December 1, 1964.

NCSL, governors and motor vehicle administrators had recommended DHS adopt a 10 year reenrollment period.

State Certification and Reporting

The final regulations create two levels of compliance for states prior to May 11, 2011: material compliance versus full compliance.

Under the material compliance threshold, a state must provide DHS with the status and operational date of state compliance with the Real ID. DHS will require states to submit a “Material Compliance Checklist.” A state must be materially compliant with the requirements of the Real ID by January 1, 2010, to receive an additional extension to May 10, 2011 date (see *State Deadlines* above).

Under the full compliance threshold, a state must meet all the requirements of the Real ID OR “have a Real ID Program that DHS has determined to be comparable to the standards” of the Real ID. A state must certify that it meets these requirements at least 90 days prior to the effective date of full compliance.

States must submit the following to DHS for review to be deemed fully compliant with the Real ID:

- A certification by the highest level Executive official in the state overseeing the Department of Motor Vehicles that reads as follows: “I, [name and title (name certifying official), (position title) of the State (Commonwealth) of _____, do hereby certify that the State (Commonwealth), has implemented a program for issuing driver’s licenses and identification cards in compliance with the requirements of the Real ID Act of 2005, as further defined in 6 CFR Part 37, and intends to remain in compliance with these regulations.”
- A letter from the state Attorney General confirming the state has the legal authority to impose the requirements necessary to meet the standards established;
- A description of the states exception process and the state’s waiver process (see below); and
- The state’s security plan.

States will have to re-certify every three years and are subject to DHS review at any time. Under the final regulations, states must provide any reasonable information to DHS “pertinent to determining compliance,” and permit DHS to “conduct inspections of any and all sites associated with the enrollment of applicants...production, manufacture, personalization and issuance of [DL] and [ID].”

Exceptions Process

NCSL, governors and motor vehicle administrators advocated for an exceptions process to address certain circumstances. Under the final regulations, states may use the exceptions process for individuals who have difficulties producing some of the required identification documents, such as proof of identity or date of birth, and must therefore rely upon other alternate documents.

Under the state’s exception process, a state must:

- Make reasonable efforts to establish the authenticity of the alternate documents;
- Maintain a record that the exception process was used in the application process;
- Retain a copy or image of the alternate documents used in the application process in the same manner as for other source documents;
- Conduct a review of the state’s exception process; and
- Provide DHS with a copy of the state’s review of its exception process as part of the state’s certification.

The exception process does not apply to precautions taken on behalf of state-issued DL and ID for federal, state and local officials, including criminal justice agencies that require safeguards due to official duties.

Funds

To date, Congress has appropriated only \$90 million to assist states with implementation of the Real ID, of which only \$9 million has been obligated. The President's FY 2006, FY 2007 and FY 2008 budget proposals did not include any funds to assist states with the implementation of the Real ID.

DHS will again enable states to use up to 20 percent of their State Homeland Security Grant Program (SHSGP) Funds for implementation of the Real ID. Under current law states are required to pass 80 percent of these funds to local governments, leaving only 20 percent for the states. This program received \$890 million in federal funds in FY 2008, which represented an increase over FY 2007 through the consolidation of the Law Enforcement Terrorism Prevention Program.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (garner.girthoffer@ncsl.org; (202) 624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

January 16, 2008

Real ID Final Regulations: Brief 2

Identification Documents, Verification Systems and Privacy

This is the second brief in a series summarizing the final regulations for implementation of the Real ID Act of 2005. In particular, this brief relates to sections of subparts B, C, and D of the regulations. Brief #3 will focus on the physical security requirements for the department of motor vehicle (DMV) facilities and background checks for DMV employees and Brief #4 will address requirements for the Real ID compliant card. The final regulations, Brief 1 and other resources on Real ID are available at: <http://www.ncsl.org/realid>

Identification Documents

Under the Real ID Act, states and territories are required to verify, with the issuing agency, the validity of the identification documents an applicant presents to establish:

- identity;
- date of birth;
- proof of social security number or that the person is not eligible for a social security number;
- the person's name and address of principal residence; and
- the person's lawful status in the United States.

The regulations define "verify" to mean authenticating that a source document is genuine and has not been altered and then validating identity data contained on the document.

An applicant would have to present at least one of the acceptable documents proposed by the Department of Homeland Security (DHS) and sign a declaration under penalty of perjury that the information presented is true and correct:

- a valid unexpired U.S. Passport (approximately 25 percent of Americans hold passports);
- a certified copy of a birth certificate;
- a consular report of birth abroad;
- a valid, unexpired permanent resident card (Form I-551);
- an unexpired employment authorization document (EAD) (Form I-766 or I-688B);
- an unexpired foreign passport with valid U.S. visa affixed accompanied by Form I-94;
- a U.S. certificate of citizenship;
- a U.S. certificate of naturalization;
- a REAL ID driver's license (DL) or identification card (ID) issued subsequent to the standards established by the regulations; or
- such other documents as DHS may designate later in the Federal Register.

States must retain a copy of the declaration and a new declaration must be signed when applicants present new source documents.

If an individual's name has changed through adoption, marriage, divorce or other court order, the individual must present documents showing the legal name change. The documents must come from a court, government agency, or other entity as determined by the state. States must maintain copies of documentation as well as a record of both the recorded name and the name on the source documents. Depending on the form in which documents are retained, states must maintain them for a minimum of seven (7) years up to a maximum of ten (10). Brief #6 will address documentation and retention in greater detail.

States can have an exceptions process for individuals who, for reasons beyond their control, are unable to present all necessary documents and must rely on alternate documents to establish identity. Alternative documents for lawful presence may only be used to demonstrate U.S. citizenship. For more on the exceptions process, see Brief #1.

Verification of Identity Documents

NCSL, governors and motor vehicle administrators recommended that states be required to employ electronic verification systems only as they become available. They also recommended that DHS prohibit federal agencies from charging states transaction fees for accessing the required systems. The final regulation calls on states to use these systems as they become available or to use alternative methods approved by DHS, and it appears that states can still expect to pay transactional access costs.

The Act contemplates that states will need to have access to 6 national databases for the purposes of verifying the validity of the required identification documents. This includes access to:

Verification System	Status
Social Security On-Line Verification (SSOLV)	Almost all states currently use this system.
Department of State	DHS is working with the Department of State to make it available.
Electronic Verification and Vital Events (EVVE)	System is currently in a pilot phase.
Systematic Alien Verification for Entitlements (SAVE)	All 50 states have Memorandums of Understanding (MOUs) for access to SAVE; however, only 20 are currently using it to verify lawful status.
Student and Exchange Visitor Information System (SEVIS)	DHS expects states to access SEVIA via SAVE, and the draft regulations suggested that connection would be in place by May 2008.
All-State DL/ID Records System	DHS issued a request for proposals largely intended to develop this system in December 2007.

DHS stated in the draft regulations that it will support the development of, but will not operate, a federated querying system, where a state could conduct all queries through one portal. State participation will be voluntary. DHS is proposing to leave the operation of this data query, including the development of the business rules, to the states. Working toward this end, on December 13, 2007 DHS published grant guidelines requesting that states submit proposals, preferably collaboratively, to develop this “hub.” Applications are due to DHS on January 28, 2008.

Verification of Address of Principal Residence

NCSL, governors and motor vehicle administrators recommended that the address of principal residence be determined by having the applicant provide an affidavit and by providing corroborating documentation.

DHS defines principal address as, “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.” DHS is requiring applicants to present at least two documents of the state’s choice that include the individual’s name and principal residence. A street address is generally required.

Verification of Birth Certificates

DHS anticipates states will be able to electronically verify the issuance of birth certificates through EVVE or another electronic system. If documents do not appear authentic or data does not match and an exceptions process is not appropriate, DHS forbids the state from issuing a REAL ID DL or ID until the information verifies. States are to refer applicants to the document's issuing agency for resolution of the match failure.

Verification of U.S. Passports or Consular Reports of Birth Abroad

It is anticipated that a state will be able to verify these documents with the U.S. Department of State or through other methods approved by DHS.

Verification of Valid U.S. Visas Affixed in an Unexpired Foreign Passport

Individuals presenting this form of documentation would require a SAVE and SSOLV check.

Verification of Lawful Status

NCSL, governors and motor vehicle administrators recommended limiting the acceptance of foreign documents to official passports accompanied by appropriate and clearly defined U.S. immigration documents. The states also recommended limiting document verification to what could be accomplished through an enhanced SAVE program that is fully developed, operational in real-time and accessible to all jurisdictions at no cost to states. The state groups also recommended the expansion of SAVE to include Certificates of Naturalization.

Verification of Social Security Number

DHS proposes allowing an applicant to establish their social security number by presenting a social security card, a W-2 form, a SSA 1099, a non-SSA 1099, or a pay stub with the applicant's name and SSN on it. An alien in the United States without authorization to work is generally not eligible for a SSN. In order to prove ineligibility for a SSN, an alien must present evidence that he or she is currently in a non-work authorized non-immigrant status. States will be required to check the validity of the number using SSOLV.

State Database and Connectivity to Other States' Databases

The regulations require a state to maintain a motor vehicle database that contains at a minimum:

- all data fields printed on the driver's license and identification cards, individual serial numbers of the card, and social security numbers;
- a record of the full legal name and recorded name (as noted above), without truncation;
- all data fields included on the machine-readable zone that are not printed on the front of the card; and
- motor vehicle driver histories, including motor vehicle violations, suspensions and points.

Prior to issuing a Real ID compliant license, states must check with all other states to determine if any state has already issued a Real ID driver's license or card to the applicant. If a state receives confirmation that the applicant holds another Real ID, the regulations require the state to confirm that the applicant has terminated or is terminating the extant Real ID pursuant to state law before issuing a new REAL ID.

DHS is exploring use of AAMVAnet or expansion of Commercial Driver's License Information System (CDLIS) or some other service as the platform for the state-to-state exchange.

Privacy

NCSL, governors and motor vehicle administrators recommended the "masking" of an address for persons in certain protected classes while securely retaining the information in the database. The state groups also recommended that the Driver Privacy Protection Act (DPPA) (18 U.S.C. Sec. 2721, etc. sec) be reconciled to reflect the new responsibilities of DMVs and advances in technology since the DPPA was passed.

The DHS privacy office issued a Privacy Impact Assessment (PIA) on the notice of proposed rulemaking (http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realidfr.pdf), which analyzed:

- concerns that the Real ID creates a national identity card or database;
- how personal information will be protected from unauthorized access or use;
- whether and how the personal information stored in digital format on the credentials will be protected against unauthorized use;
- the use of a photograph and address on the credential; and
- the requirement that DMVs conduct a financial history check on covered employees.

In response to these concerns, the DHS privacy office issued a PIA on the final rule. The PIA explains how the final rule addressed the concerns of the initial PIA. A copy of the report can be accessed at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realidfr.pdf.

NCSL has identified a number of provisions in the final regulations that remain of interest as they relate to the protections of individuals' identity.

Security Plan/Certification

A state's security plan, as submitted for certification, is required to outline how it will protect the privacy of personally identifiable information collected, disseminated or stored. States must establish a privacy policy regarding personally identifiable information collected and maintained by the DMV. The regulations set the Driver's Privacy Protection Act as the floor for use of personal information collected by DMVs, but states may set more stringent requirements, which will not be subject to DHS review.

Protection of Information Contained in Machine Readable Zone (MRZ) of the Card

At this time, DHS is not requiring the encryption of the information contained in the MRZ of the card. States are required to use a PDF417 2D bar code, with the following defined minimum data elements – expiration date, full legal name, transaction date, date of birth, gender, address as listed on card, unique identification number, revision date, inventory control number of the physical document, and state or territory of issuance.

Masking the Address for Persons in Certain Protected Classes

States are not required to comply with certain requirements when issuing driver's licenses or identification cards in support of federal, state or local criminal justice agencies or programs that require special licensing and safeguards. These cards must not be distinguishable from other Real ID licenses or cards issued by a state.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

January 16, 2008
Real ID: Brief 3

Physical Security of DMV Facilities and Databases; DMV Employee and Applicant Background Checks

This is the third brief in a series summarizing “Subpart D” of the final regulations for implementation of the Real ID Act of 2005. Brief 4 will focus on the physical security features of the Real ID card. A copy of the final regulations and other NCSL resources on Real ID, including other briefs, are available at: <http://www.ncsl.org/realid>

Physical Security of DMV Facilities and Databases

Under the Real ID Act, a state must ensure “the physical security of locations where drivers’ licenses (DL) and identification cards (ID) are produced and the security of document materials and papers from which DLs and IDs are produced.”

NCSL, governors and motor vehicle administrators recommended that facility-based risk assessments and mitigation plans be included as part of a state’s self-certification process (for additional information on state self-certification, see Brief #1).

State Security Plans

The final regulations require that a state’s comprehensive security plan address:

- the physical security of the facilities used to produce and store materials used in Real ID card production;
- the security of personally identifiable information maintained at Department of Motor Vehicles (DMV) locations;
- documents and physical security features of Real ID cards (see *Brief #4*);
- access controls for DMV employees and contractors, including:
 - employee identification and credentialing,
 - employee background checks, and
 - controlled access systems;
- periodic training requirements for employees, including fraudulent document recognition programs and security awareness training;
- emergency/ incident response plans;
- internal audit controls; and
- an affirmation that the state has the authority and means to protect the confidentiality of persons issued Real ID compliant ID and DL in support of federal, state and local criminal justice agencies, or special licensing or identification programs to safeguard ID holders in their official capacity.

Physical Security Requirements of Real ID Facilities and Storage Areas

States must take measures to ensure the physical security of facilities used in the manufacture and issuance of Real ID-compliant DLs and IDs, however, DHS does not stipulate the manner in which a state secures its facilities.

Security of Personally Identifiable Information

The regulations stipulate that states must take reasonable efforts to protect the personal information used to comply with the requirements of the Real ID, including protections to prevent unauthorized access, use or dissemination of such information. State security plans must detail policies and procedures for document retention and destruction; states must also institute a privacy policy for information collected and maintained by the DMV under the requirements of the Real ID. In addition, states must maintain minimum protections regarding the release and use of personal identifiable information under existing federal law (contact NCSL for more information).

Employee Background Checks

Under the Real ID Act, a state must ensure that “all persons authorized to manufacture or produce drivers' licenses and identification cards [are subject] to appropriate security clearance requirements.”

NCSL, governors and motor vehicle administrators recommended that states be allowed to:

- identify those staff (employee/vendor/contractor) involved in the manufacture and production of DLs and IDs who require security clearance, as part of the state’s self-certification;
- subject employees to a minimum of a state and federal background checks;
- grant new hires provisional clearance pending results of a background check ;
- enumerate disqualifying criteria in the state self-certification, as well as procedures for interim hiring pending results of background checks; and
- have a means to deal with the realities of operative personnel laws, regulations and labor relations agreements applying to pre-existing employees.

Under the final regulations, states must conduct background checks on:

- all persons involved in the manufacture or production of a Real ID compliant DL and ID;
- persons that may affect the information on a Real ID compliant DL and ID; or
- current employees or contractors that will be assigned to such positions, or a “covered employee” that meets the first two qualifications.

“Covered employees” are defined as “DMV employees or contractors who are involved in the manufacture or production of Real ID [DL] or [ID], or who have the ability to affect the identity information that appears on the [DL] or [ID].”

Each state will determine which applicants, employees or contractors will be subject to the background check. States will also be required to provide notice to the applicant, employee and contractor that a background check will be conducted.

The background check must include, at a minimum:

- a validation of references from prior employment;
- a name-based and fingerprint-based criminal history records check through the state and two FBI's databases—National Crime Information Center(NCIC) and Integrated Automated Fingerprint Identification System (IAFIS) (at the cost of the state); and
- employment verification as otherwise required by law.

However, background checks substantially similar to the requirements of the regulations do not have to be repeated if conducted on or after May 11, 2006.

The regulations established a bifurcated system for disqualifying an applicant for employment due to a criminal history. Under a “permanent disqualifying criminal offenses,” any “covered” applicant, existing employee or contractor is disqualified from employment if the employee or applicant is convicted of certain felonies (for more details contact NCSL).

Under a “interim disqualifying criminal offenses,” a “covered” applicant, employee or contractor may also be disqualified, absent a state adopting a waiver process, if:

- convicted of a disqualifying offense within 7 years of the date of employment;
- released from incarceration within 5 years of the date of employment; and
- under a felony warrant until the warrant is released.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

January 18, 2008

Real ID: Brief 4

Requirements for the Real ID Compliant Card

This is the fourth brief in a series summarizing the regulations for implementation of the Real ID Act of 2005. This brief relates to several sections of subpart B of the regulations, which focus on the features of the Real ID card. Brief 5 will address regulations for the non-compliant card and temporary cards. A copy of the regulations and other NCSL resources on the Real ID, including other briefs, are available at: <http://www.ncsl.org/realid>

Minimum Data Element Requirements

The Real ID Act prescribes that a certain set of information and features appear on Real ID compliant, state-issued driver's licenses (DL) and identification cards (ID). The law stipulates the following nine as minimums:

1. The person's *full legal name*;
2. The person's *date of birth*;
3. The person's *gender*;
4. The person's DL or ID *number*;
5. A *digital photograph* of the person;
6. The person's *address of principal residence*;
7. The person's *signature*;
8. *Physical security features* designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes; and
9. A common *machine-readable technology*, with defined minimum data elements.

NCSL, governors and motor vehicle administrators made a number of recommendations addressing data element requirements. They include: requiring the capture of up to 125 characters for full legal name; requiring the federal government to adopt and universally apply common naming conventions to its systems; and, with input from states, developing and applying naming truncation guidelines to all systems accessed under the Real ID. In addition, states recommended that the regulations provide states the necessary flexibility to engineer their system and business processes as it relates to the capture of facial images as long as the image is captured when a DL/ID is issued and before a credential is denied.

The regulations detail the statutorily included nine elements that must be included on the face of the Real ID and add the following to the list:

10. *Issue date*;
11. *Expiration date*;
12. *State or territory of issuance*; and
13. *DHS approved security marking*.

The *full legal name* for the Real ID card must be identical to the name shown on the identity document used to obtain the DL/ID (see Brief 2 for more on identity documents). Any name variations due to marriage, divorce, adoption, or court order must be documented. States must maintain a complete record of an individual's name history. The regulations adopt the International Civil Aviation Organization (ICAO) 9303 Standard for the name as it will appear on the face of the DL/ID. This standard requires Latin alphabet characters, allows a total of 39 characters on the face of the card, and provides standards for truncation of longer names.

Each DL/ID must display a unique *card number*. As federal law prohibits the display of a person's Social Security Number (SSN) on a DL, states must generate a different and unique document number.

States must capture a full facial *digital image* of everyone applying for a DL/ID. If a DL/ID is issued, the image must appear on the face of the card; photographs may be black and white or color. If a DL/ID is not issued, DHS requires that states retain the image for at least five years, regardless of the reason for non-issuance. Digital photographs should comply with ICAO standards, including diffused lighting over the full face eliminating shadows or “hotspots,” a full face image from the crown to the base of the chin and from ear-to-ear, and prohibition of veils, headdresses or eyewear that obscure facial features or the eyes or create shadows. DHS contends that the law makes no allowances for the exclusion of facial photographs based on religious or other beliefs, but states may issue non-compliant DL and ID in such cases. An applicant’s photo should be taken upon reapplication, but not less frequently than every 16 years.

The person’s *address of principal residence* must appear on the face of the card. Conforming to recommendations from NCSL, governors, and motor vehicle administrators, the regulations allow for a state exemption processes for confidential addresses (of judges, victims of domestic violence, protected witnesses, etc.) and applicants with no fixed address be continued.

The person’s *signature* must meet the size, scaling, cropping, color, borders, and resolution requirements stated in existing American Association of Motor Vehicle Administrators (AAMVA) standards.

The regulations require states to use the existing AAMVA standard 2D bar code for the *machine-readable technology* on the card. DHS requires that the PDF-417 2D bar code approved by AAMVA store the minimum data elements – expiration date, bearer’s name, issue date, date of birth, gender, address, unique DL/ID number, DL/ID format revision date, inventory control number, and state or territory of issuance. DHS is not requiring encryption of this machine-readable information.

The card shall also include a *DHS approved security marking* to indicate the card’s level of compliance with the Real ID— full v. material compliance (see Brief #1).

Physical Security Features

The Real ID Act requires states to utilize multiple layers of *physical security features* on a DL and ID that are not reproducible using commonly used or available technologies in order to deter forgery and counterfeiting and to promote an adequate level of confidence in the authenticity of the document.

NCSL, governors and motor vehicle administrators recommended that the regulations establish performance requirements for DL/ID cards rather than mandating use of a specific set of security features. Recommendations also included initiating an advisory group composed of document security experts from federal and state agencies to establish national performance criteria and creating a testing program, in cooperation with states, to determine the resistance of DL/ID cards to tampering, counterfeiting or duplication for fraudulent purposes.

The final regulations require states to employ three levels of card security features for Real ID compliant DL/ID:

- Level 1 must provide for easily identifiable visual or tactile features to allow a cursory examination for rapid inspection;
- Level 2 provides for an examination by trained inspectors with simple equipment; and
- Level 3 provides for inspection by forensic specialists.

For example, a state would choose several features, such as tamper-proof printed information, an optically variable feature or an ultraviolet (UV) responsive feature, and satisfy each level of security required under the final regulations.

However, the regulations do not mandate specific security features or card stock for DL/ ID cards. States must conduct a review of it’s DL/ID design and submit a report to DHS that indicates the ability that the card design is resistant to compromise and document fraud. DHS may request an independent laboratory conduct analysis regarding the card’s security features. States must also notify DHS whenever a security feature is modified, added or deleted.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org; (202) 624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

January 21, 2008

Real ID Final Regulations: Brief 5

Non-Compliant and Temporary Driver's Licenses and Identification Cards

This is the fifth brief in a series summarizing the final regulations for implementation of the Real ID Act of 2005. This brief focuses on the non-compliant and temporary driver's licenses (DLs) and identification cards (IDs) and relates to sections of Subparts B and F of the regulations. Brief 6 will focus on document and record retention. The final regulations, prior briefs, and other resources on Real ID are available at <http://www.ncsl.org/realid>.

Non-Compliant Real ID Driver's License and Identification Cards

The Real ID Act itself stipulates that a state complying with REAL ID that also issues non-compliant DLs and IDs must:

- clearly state on the face of the DL/ID that it may not be accepted by any federal agency for federal identification or any other official purpose; and
- use a unique design or color indicator to alert federal agency and other law enforcement personnel that the DL/ID may not be accepted for any such purpose.

NCSL, governors and motor vehicle administrators recommended that the regulations allow states to meet the requirement at reduced cost by placing a restriction code on the front of license, with clarifying language on back.

DHS is requiring that the card clearly states on its face and in the machine readable zone that it may not be accepted by any federal agency for federal identification or any other official purpose. DHS is also requiring states to incorporate a unique design or color indicator to distinguish it from the state's REAL IDs and to alert federal agencies and other law enforcement personnel that it may not be accepted for federal purposes. DHS reserves the right to approve the non-compliant cards designations during the state compliance certification process.

Temporary Driver's Licenses and Identification Cards

Under the Real ID Act, a state must issue a temporary or limited-term DL or ID if an applicant has temporary lawful status and provides evidence, verifiable through SAVE or another DHS-approved method, by presenting one of the following:

- a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States;
- a pending application for asylum in the United States;

- a pending or approved application for temporary protected status in the United States;
- approved deferred action status; or
- a pending application for adjustment of status to that of an alien lawfully admitted for permanent residence in the United States or conditional permanent resident status in the United States.

Temporary or limited-term DLs and IDs must clearly indicate on the face of the card and in the machine-readable zone that they are temporary. The law stipulates that the date on which a temporary DL/ID expires must also be clearly indicated (see NCSL Brief #4). The temporary DLs and IDs may only be valid for the time period of the applicant's authorized stay in the United States, but not longer than the state's maximum DL/ID term. If there is no definite end period for the authorized stay, then the DL/ID shall be good for a period of one year.

A state may not reissue a temporary DL/ID unless the document of lawful presence has been extended by DHS or the person has qualified for another lawful status. A renewal of a temporary DL/ID must be in person.

NCSL, governors and motor vehicle administrators recommended that the regulations needed to clarify that the requirements of this provision apply to those deemed temporary due to limited duration of lawful presence, rather than other state-issued "temporary" licenses (e.g. medical restrictions, etc.). It was also recommended that the minimum requirement for identifying restricted license duration should be indicated as a restriction code on the front of the license, with clarifying language on back, as is standard for other license restrictions.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

January 21, 2008

Real ID Regulations: Brief 6

Document and Record Retention

This is the sixth brief in a series summarizing the final regulations for implementation of the Real ID Act of 2005. This brief relates to a section of subpart C of the regulations, which focuses on the document and record retention requirements of the final regulations. Brief 7 will address regulations for the renewal and re-issuance process for Real ID compliant driver's licenses (DL) and identification cards (ID). A copy of the regulations and other NCSL resources on the Real ID, including other briefs, are available at <http://www.ncsl.org/realid>.

Under the Real ID Act, states are required to retain copies or images of source documents for issuance of Real ID compliant DL and ID. Copies of source documents must be retained for at least 7 years; images of source documents must be retained for at least 10 years.

NCSL, governors and motor vehicle administrators recommended that the states not be required to capture documents presented by an applicant to verify address of principal residence. It was also recommended that DHS clarify the need for and ability of states to electronically transfer source documents.

Under the regulations, DHS requires states to retain copies of the following documents:

- signed declaration affirming that the information presented by the applicant is true and accurate as required under state law;
- an original or certified copy of identity documents or source documents, such as a birth certificate or passport (see NCSL Brief #2);
- if applicable, the alternate documents used to demonstrate a name change as permitted under state law;
- if applicable, the alternate documents accepted or copies thereof used under a state's exceptions process (see NCSL Brief #1); and
- digital photograph of the applicant or cardholder (also see NCSL Brief # 4).

A state must also describe its standards and procedures for safeguarding and destroying source documents in the state's security plan (see Brief #8).

The regulations require that states retain:

- paper copies of source documents for a minimum of 7 years;
- microfiche copies of source documents for a minimum of 10 years;
- digital images of a source documents for a minimum of 10 years; AND
- digital photograph of the cardholder for at least 2 years beyond the expiration of the card; OR
- digital photograph of the applicant (if a DL/ID is not issued) for at least 5 years.

States that choose to store source documents in a digital format must:

- store photo images in Joint Photographic Experts Group (JPEG) 2000 format, or standard that is interoperable with this format;
- store document and signature images in a compressed Tagged Image Format (TIF), or a standard that is interoperable with the TIF standard;
- ensure all images are retrievable if properly requested by law enforcement; and
- upon request by the DL/ID applicant, record and retain the applicant's birth certificate information in lieu of an image or copy thereof.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

February 8, 2008

Real ID Final Regulations: Brief 7

***Renewal and Reissuance Process for Real ID Compliant
Driver's Licenses and Identification Cards***

On January 11th, the Department of Homeland Security (DHS) issued the long-awaited final regulations for implementation of the Real ID Act of 2005. This is the seventh brief in a series summarizing the rules and processes for renewing and reissuing Real ID driver's licenses (DL) and identification cards (ID). It relates to sections of Subpart B of the regulations. Brief 8 will focus on state security plans and reporting requirements. The final regulations, prior briefs, and other resources on Real ID are available at <http://www.ncsl.org/realid/>.

Renewal and Reissuance of Real ID Compliant Cards

The regulations define a "reissued card" as a card that a state DMV issues to replace a card that has been lost, stolen, or damaged or that contains outdated information. A "renewed card" is a DL or ID that a state issues to replace a renewable DL or ID, presumably on or around the date of expiration.

The Real ID Act limits the period of validity of all Real ID DL/ID cards that are not temporary to a period not to exceed eight years. While states can have validity periods of less than eight years, an individual must apply for a renewal in person at a DMV office at least every 16 years. At least every 16 years, the DL/ID photograph must be updated, the applicant's Social Security number and lawful status must be reverified, and the state must electronically verify any other information that it was not previously able to verify (due to system unavailability or for other reasons).

For renewals between the initial issuance of a Real ID and that occurring in the 16th year, states may establish procedures to permit remote (or "non-in-person") renewals. Social Security numbers and lawful presence must be reverified and there can be no "material change" in any of the personally identifiable information (see Brief #2). A change in address of principal residence, however, does not constitute a "material change."

Renewal and Reissuance of Temporary Cards

States must verify lawful status via the Systematic Alien Verification for Entitlements system (SAVE) or another method approved by DHS before renewing or reissuing temporary or time-limited Real ID DL/ID. (see Brief #2)

Renewal and Reissuance of Non-Compliant Cards

The renewal process of non-Real ID compliant DL/ID cards is not subject to the regulation.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).



Information Alert

National Conference of State Legislatures
Office of State-Federal Relations

February 13, 2008

Real ID Final Regulations: Brief 8

State Security Plans and Reporting Requirements

This is the eighth brief in a series summarizing the final regulations for implementation of the Real ID Act of 2005. This brief relates to sections of subpart B, D and E of the regulations, which focus on state security plans and other reporting requirements as outlined in final regulations. A copy of the regulations and other NCSL resources on the Real ID, including other briefs, are available at <http://www.ncsl.org/realid>.

Under the Real ID Act, the Secretary of the Department of Homeland Security may prescribe the requirements of a state's self-certification request to comply with the Real ID. (see Brief #1)

The final regulations require states to submit a security plan in conjunction with a state's certification. At a minimum, state security plans must address:

- the physical security of the facilities used in the production and storage of Real ID cards;
- the security of personally identifiable information collected, stored, accessed or disseminated by DMV, including a privacy policy regarding personally identifiable information;
- the document and security features of a Real ID compliant card, including the state's use of biometrics and standards utilized;
- access controls for employee credentialing, employee background checks and controlled access to various systems utilized in the production of a Real ID;
- state training programs for fraudulent document recognition, threat identification and the handling of sensitive security information;
- a state's emergency and incident response plan;
- a state's internal audit controls; and
- a state's affirmation to protect the confidentiality of card holder information issued in support of federal, state and local criminal justice activities or protection of the identity of persons serving in an official capacity.

A state security plan must be handled and protected in accordance with federal standards for sensitive security information as determined by the Department of Transportation (see [49 CFR 1520](#)).

State Reporting Requirements

If applicable, states must also provide the Department of Homeland Security (DHS) with the following:

- state request for an extension of the Real ID requirements deadline (see Brief #1);
- state certification documentation (see Brief #1);
- documentation of any exceptions and waiver procedures (see Brief #1); and
- state report(s) on a state's card security evaluation (updated with any security feature modification change)(see Brief #4).

If applicable, a state may also reply to a preliminary DHS finding of non-compliance under the state certification process. The state reply must include an explanation of any corrective action to remedy non-compliance or provide a detailed analysis of why a finding of non-compliance was incorrect. A state's reply must be filed within 30 days of a DHS finding of non-compliance.

For more information contact NCSL staff Jeremy Meadows (Jeremy.Meadows@ncsl.org, 202-624-8664) or Garner Girthoffer (Garner.Girthoffer@ncsl.org, 202-624-7753).