Privacy Impact Assessment
for the

REAL ID Act

In conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes

March 1, 2007

Rulemaking Contact Point
Darrell Williams
REAL ID Program Office
Department of Homeland Security
Washington, DC 20528
(202) 282-9829

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813
privacy@dhs.gov

Abstract

The Department of Homeland Security (DHS) Privacy Office is conducting a Privacy Impact Assessment (PIA) on the rule proposed by DHS to implement the REAL ID Act. The authority for this PIA is Subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which calls for the Chief Privacy Officer of the Department of Homeland Security (DHS) to conduct a "privacy impact assessment of proposed rules of the Department." This analysis reflects the framework of the Privacy Office's Fair Information Principles, which are: Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The Privacy Office conducts PIAs, whether under Subsection 4 of Section 222 or under Section 208 of the E-Government Act, to ensure that DHS is fully transparent about how its proposed rules, final rules, and intended information technology systems may affect privacy and to review alternative approaches and technologies that may minimize the privacy impact on individuals. This PIA examines the manner and method by which the personal information of American drivers and identification (ID) holders will be collected, used, disseminated, and maintained pursuant to the proposed rule issued under the REAL ID Act. This PIA will be updated, as necessary, when the rule is final.

Introduction

This PIA is prepared pursuant to Subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which calls for the Chief Privacy Officer of DHS to conduct a "privacy impact assessment of proposed rules of the Department."[1] Section 208 of the E-Government Act (Public Law 107-347) also provides for PIAs for all new or substantially changed technology that collects, maintains, or discloses personal information. Distinct from the PIA required under Section 208, Subsection 4 of the Homeland Security Act authorizes the Chief Privacy Officer to conduct a privacy impact assessment of proposed departmental regulations, which may or may not involve a particular technology system. The authority under Subsection 4 is significant since a proposed rule may raise privacy considerations regarding information practices that do not involve technology or a proposed rule may address technology systems that the Department does not own or control. Therefore, Subsection 4 provides the Chief Privacy Officer with the broadest authority to identify and comment on privacy matters resulting from proposed departmental regulations and to do so in a manner that is public.

This PIA examines the manner and method by which the personal information of American drivers and ID holders will be collected, used, disseminated, and maintained pursuant to the proposed rule promulgated under the REAL ID Act (the Act).[2] This analysis reflects the framework of the Privacy Office's Fair Information Principles, which are: Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. This PIA will be updated, as necessary, when the rule is final.

The Notice of Proposed Rulemaking (NPRM) establishes minimum standards for state-issued driver's licenses and identification cards that federal agencies will accept for "official purposes" after May 11, 2008.

---

[1] Homeland Security Act of 2002, 6 U.S.C. § 142(4), Pub. L. 107-296, 116 Stat. 2135, 2155 (November 25, 2002), as amended ("(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected").

[2] Division B—REAL ID Act of 2005, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13, 119 Stat. 231, 301 (2005) (codified at 49 U.S.C. 30301 note).

Specifically, the Act mandates minimum document and information verification requirements, security features, physical security standards for locations that issue driver's licenses and identification cards, and background checks for Department of Motor Vehicle (DMV) employees who have the ability to affect the identity information that appears on the credentials, have access to the production process, or are involved in the manufacturing of the credentials (covered employees). In addition, the NPRM provisions call for security standards to ensure that the valuable information state DMVs collect will be protected and not used as a source for identity fraud or theft.

The Act and its proposed implementing regulation will result in issuance of credentials that are tamper-resistant and better identity documents than the current driver's license and identification card issued by the states. A better credential should help address the use of falsified credentials in perpetrating identity theft. In addition, as a result of the Act, state databases will contain standardized photo images that will allow law enforcement agencies to use facial-recognition technology to help apprehend criminals, and the state DMVs will be able to use the images and application data to prevent drivers whose licenses have been revoked in one state from obtaining them in another.

This PIA analyzes the major privacy concerns posed by the Act and addressed in the NPRM. The first and overarching concern is whether the Act and the implementing regulations will result in the creation of a national identity card or database. The second is whether and how the personal information associated with implementation of the Act will be protected from unauthorized access or use. The third is whether and how the personal information stored in digital format on the credentials will be protected against unauthorized uses. This PIA discusses several additional privacy issues that were not raised in the Privacy Considerations section of the NPRM, including the proposed requirements that a photograph and address appear on the credential and that DMVs conduct a financial history check on covered employees.

The Privacy Office strongly supports the application of the privacy protections discussed in the NPRM to protect the personal information associated with REAL ID driver's licenses and identification cards stored in state databases and encourages public comment on the privacy and security issues posed at the conclusion of the Privacy Considerations section of the NPRM including: state comprehensive security plans; access to information collected by states pursuant to the REAL ID Act and the protection of such information stored in state databases; and the operation and governance of electronic verification by states of driver's license application information.

The Privacy Office recommends that the final rule continue to address privacy issues clearly and that it define sufficient privacy protections to ensure that DHS can audit and certify their implementation by the states. Moreover, as discussed below in Section II.C. of this PIA, to the extent technically and operationally feasible, the Privacy Office believes there is a strong privacy rationale for cryptographic protections to safeguard the personal information stored digitally in the machine-readable zone (MRZ) on the credentials.

I. Legislative History

The Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005[3] contained the provisions for the REAL ID Act of 2005, which repealed the driver's licensing section of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[4] While the REAL ID Act does not contain an explicit requirement that DHS enact rules to protect the privacy rights of individuals

[3] Pub. L. 109 -13, 119 Stat. 231, 302 (2005)(codified at 49 U.S.C. § 30301 note).
[4] Pub. L. 108-458, 118 Stat. 3638, 3827 (December 17, 2004)(codified at 49 U.S.C. § 30301 note).

who apply for and hold driver's licenses and personal identification cards, the legislative history of the Act supports the conclusion that Congress intended DHS to do so. The House Conference Report for the REAL ID Act includes several key statements of Congressional intent regarding privacy.[5] For example, in its discussion of section 202(d)(12) of the Act, which requires each state to provide electronic access to the information in its motor vehicle databases to all of the other states, the Conference Report makes clear that Congress recognized the need for the regulations to address privacy and security and that those protections should be at least the equivalent of existing federal protections. The Conference Report reads in relevant part:

> *DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards which meet the standards for federal identification and federal purposes.*[6]

In addition, the Conference Report discussion of Section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," clearly indicates that Congress wanted privacy to be a consideration in implementing the technology. The Conference Report states:

> *There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement officials."*[7] *(Underlining for emphasis, not in the original)*

This statement suggests that Congress wanted to secure the privacy of the data contained on the machine readable zone (MRZ) of the credential and make it accessible only to law enforcement officials. The current understanding is that a potential way to control access to the data on the 2D bar code by third parties, which is the technology DHS has selected to be used in the REAL ID credentials, is encryption. The issue of how to protect this information is discussed in Section II.C. of the PIA, below.

The Conference Report language described above, coupled with the requirement in Section 202(d)(7) of the Act to "ensure the physical security of locations where driver's licenses and identification cards are produced and the security of document materials and papers from which driver's licenses and identification cards are produced," provide the legislative basis to include privacy protections and safeguards for both the personal information collected and used in connection with the issuance of REAL ID driver's licenses and identification cards and the personal information stored on these credentials.

II. The Privacy Impact of the REAL ID Act and the NPRM

The public has long been accustomed to providing personal information for the purpose of obtaining driver's licenses and identification cards. This includes having this information printed on the face of these credentials and, in most states, included in a machine readable technology (MRT), such as a bar code or magnetic strip on the rear of the credential. The enactment of the REAL ID Act increases the attention on the privacy ramifications of what information will appear on the driver's licenses and identification cards issued under the Act and the privacy of the information that will be exchanged. Some privacy advocates and members of the public have raised concerns that the Act could create an increased risk of identity theft

---

[5] H.R. Rep. No 109-72 (2005) (Conf. Rep.)
[6] Id. at 184. .
[7] Id. at 179.

and erode privacy or be a stepping-stone to a national identity card, because of the standardization of the information that will be presented on the credential, the uniformity of the process for issuance of the credentials, and potential federal access to the mandated information.

As described below, DHS has sought to address the privacy concerns within the limits of its authority under the Act.[8] At the federal level, only the Driver's Privacy Protection Act of 1994 (DPPA)[9] addresses the privacy of motor vehicle records, but as described below in Section II.B. of the PIA, its protections are narrowly focused. It is therefore necessary to build federal protections into the REAL ID rulemaking to augment existing state administrative and statutory privacy protections. This section of the PIA summarizes the requirements of the Act that potentially have the greatest impact on privacy, the extent to which those requirements change current state driver's licensing practices, and how DHS intends to address concerns that the Act will result in a national identity card or database and erode privacy. The privacy concerns surrounding a national identity card stem from the REAL ID Act itself and not from DHS's proposed rulemaking, because DHS does not have authority to control third-party use or potential use of the REAL ID credential or associated identifier.

The PIA addresses the key privacy issues posed by the Act: (1) Does the REAL ID Act create a national identity card or database; (2) How will personal information required by the REAL ID Act be protected in the state databases; (3) How will the personal information stored on the machine readable technology on the driver's licenses and identification cards be protected from unauthorized collection and use; and (4) Do the requirements for a photograph and address on the credential and the DMV employee background check erode privacy.

A. Does the REAL ID Act create a national ID or database?

The overarching privacy concern regarding the Act is that it will create a national ID or database on all driver's license and identification card holders. The Privacy Office is mindful of Congress's views on national identification cards, expressed in Section 1514 of the Homeland Security Act of 2002.[10] This PIA discusses both the issue of a national identity card/number and the issue of a national database, as they are related but not identical concerns. First, it is yet unclear whether a REAL ID compliant driver's license or identification card will become any more of a national ID than the Social Security Number (SSN) or existing state-issued driver's licenses and identification cards. An argument exists that both the SSN and existing state credentials already create *de facto* national identifiers. Nevertheless, it is likely that given the stringent verification process to obtain a REAL ID credential and the security features proposed in the NPRM to prevent credential counterfeiting and tampering, the REAL ID credential may soon be considered the most reliable credential to ascertain an individual's identity.

Nonetheless, it is important to understand whether and how the Act may change the use of driver's licenses by the public and private sectors Although the REAL ID Act will make the driver's license and number a more reliable identifier, it is not yet clear to what extent it will expand the use of the license or number.

---

[8] DHS has taken steps to protect privacy pursuant to its authority under Section 202(d)(7) to address the security of the information DMVs will collect and use related to implementation of the Act and its authority to define the machine-readable technology. This is consistent with the House Conference Report (*See* H.R. Rep. No 109-72 at 179, 184 discussing section 202(b)(9) [the machine-readable technology] and 202(d)(12) [the state data exchange] of the Act.

[9] Pub. L. 103-322 as amended by Pub. L. 106-69, 18 U.S.C. § 2721 et seq.

[10] Section 1514 states the following: "Nothing in this Act shall be construed to authorize the development of a national identification system or card."

The REAL ID Act, however, does not limit the ability of Congress or the states in the future to restrict the use of the REAL ID or its unique number beyond the uses specified in the Act and the proposed regulations. Although DHS is mindful of these issues, the future use of the new credential by third parties and not this rulemaking will ultimately determine whether the REAL ID credential will become a national ID and whether further protections from Congress may be warranted.

1. Use of a Unique Identifier

Third parties such as financial institutions, retailers, hotels, health-care providers, and others may consider the REAL ID credential to be a more reliable identification card than existing credentials, including current driver's licenses, and may begin to request this credential in conjunction with a wide variety of transactions, including applications for employment, opening credit or other accounts, making credit purchases, or other transactions in which it is necessary to ascertain the identity of the individual involved in the transaction. This could be helpful in reducing the incidence of fraudulent face-to-face transactions, but only if the third party actually compares the information on or associated with the credential with the individual presenting it, such as examining the signature or photograph of the individual. A REAL ID credential, however, cannot provide assurance of identity for transactions that take place remotely on the Internet or by phone.

The NPRM limits the scope of "official purposes" of the credential to the uses specified in the REAL ID Act: (1) accessing federal facilities; (2) boarding federally-regulated aircraft; and (3) entering nuclear power plants.

All identity systems trigger privacy concerns and extend not only to the use of a credential, but to the use of any unique number associated with the credential. Section 202(b)(4) of the REAL ID Act requires that each REAL ID driver's license or identification card include the person's unique "driver's license or identification card number." For privacy reasons, federal law already prohibits the display of an individual's SSN on a driver's license,[11] but the unique ID number on a REAL ID credential, if left unregulated, could be misused in similar ways. This is a risk inherent to the law enacted by Congress and the proposed implementing regulations cannot ameliorate this risk. Thus, for example, if retailers, healthcare providers, financial institutions, insurers, and other private or government entities were to collect the credential and record the ID number whenever individuals engaged in a transaction, the REAL ID's unique number could pose the same, if not greater, risks as experienced in the use of the SSN.[12]. As discussed in Section II.C. below, the collection of personal information from the credential could be further facilitated by the skimming of the digital information stored in the MRZ if it is not encrypted or such actions are not prohibited by law.

Our system of government with its checks and balances can prevent such an erosion of privacy and civil liberties, if protections are built into the identity system from the very beginning. Of course, unlike a SSN, a person's driver's license number may change over time if the person moves from one state to another. Moreover, even under the REAL ID Act, Congress and state governments always retain the ability to restrict the use of a REAL ID as a unique identifying number in the future if warranted.

---

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

[12] The risks associated with the SSN are increasingly being addressed through legislation to limit its use, such as Section 7214 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, December 17, 2004, preventing its display on driver's licenses.

Some of the public concern about the REAL ID stems from the history surrounding the expansive use of the SSN beyond its original purpose of recording the information necessary to provide a public pension benefit. One of the lessons learned from the use of SSNs is that once an identification number is issued, it is very difficult to limit its use.[13] A National Academy of Sciences National Research Council study of identification systems, *IDs – Not That Easy: Questions About Nationwide Identity Systems,*[14] posed serious concerns about the desirability and feasibility of a nationwide identity system. The study noted that any identity system raises significant and challenging policy, procedural, and technological issues and urged policymakers to consider a set of key questions when contemplating an identity system. This study proposed the following questions, which are appropriate to consider at this early stage of addressing the REAL ID Act: What is the purpose of the system? What is the scope of the population that would be issued an ID and recorded in the system? What is the scope of the data? Who would be the users of the system? What types of use would be allowed? Would participation be voluntary or mandatory? What legal structures protect the system's integrity as well as the data subject's privacy and due process rights, and determine the government and relying parties' liability for system misuse or failure?

Even now, over 70 years after the SSN was first introduced, the federal government is grappling with how to address the privacy and security interests surrounding the role of SSNs in facilitating identity theft. While DHS believes the issuance of REAL ID credentials can help reduce the incidence of identity theft, it is unclear whether a unique identifier associated with the REAL ID credential will over time suffer the same problems as those associated with the SSN. The only way to prevent misuse of any identifier is to establish enforceable restrictions at the time any REAL ID identifier is introduced. For a number of years, many bills have been proposed in the Congress to address misuse of the SSN; however, none have been passed because it is a challenge to limit the use of the SSN now that it has become such a common identifier in the marketplace.

Although DHS cannot address all of these concerns about a national ID or the use of the unique identification number because DHS can only act within the authority granted under the REAL ID Act, DHS can play an important role in eliminating the concern that implementation of the Act would result in the creation of a national database. The NPRM does not propose to create a national database. This concern stems from the provisions in the Act requiring that the individual states: (1) electronically verify application information against federal databases; and (2) provide state-to-state access to verify that the applicant only holds a valid driver's license or identification card in one jurisdiction. Furthermore, storing personal information in a uniform and standardized manner, such as the information on individuals possessing REAL ID credentials, poses a significant security risk given the value of this collection of information. Consequently, the Privacy Office recommends that states, with participation of the affected federal agencies, develop and implement a governing structure to devise the business rules and requirements that apply to the operation of both the state-to-federal data query and the state-to-state data exchanges. This concept would be substantially similar to current governance practice in the issuance and management of state driver's licenses and identification cards.

As discussed below, an architecture for implementing the mandated data verifications and exchanges can be designed, governed, and operated to avoid the creation of a national database. The key will be to ensure that the states administer and manage the systems built to implement the Act. In addition, with appropriate

---

[13] *See* GAO Reports on SSNs: GAO-02-352, GAO-05-1016T,

[14] Stephen T. Kent and Lynette I. Millett (Editors), *IDs—Not That Easy: Questions About Nationwide Identity Systems*, National Academy of Sciences (2002)

and necessary participation from the affected federal agencies, including DHS, the Department of Transportation, and the Social Security Administration, the states must be empowered to develop the business rules surrounding the check of federal reference databases and the state-to-state data exchange processes. State, rather than federal, operation and control of the systems not only minimizes the appearance of a national database, but also fosters the system of federalism upon which our country is based.[15] The language in the Preamble of the NPRM supports the important role of the states.

2. The State Query of Federal Reference Databases

Section 202(c)(3)(A) of the REAL ID Act requires a state before issuing a driver's license or identification card to verify with the issuing agency the issuance, validity, and completeness of each document required to be presented. It is difficult to validate that source documents, such as a birth certificate, Permanent Resident Card, and foreign passport with a valid unexpired U.S. visa, are genuine and have not been altered. The proposed regulation contemplates that certain identifying data contained in source documents will be checked electronically against federal reference databases. Specifically, states may be required to verify the data within the source documents against the following federal databases:

- Systematic Alien Verification for Entitlements (SAVE) database operated by DHS U.S. Citizenship and Immigration Service (USCIS);[16]
- Social Security On-Line Verification (SSOLV) database operated by the Social Security Administration (SSA);
- Electronic Verification of Vital Events (EVVE) database, the birth certificate verification pilot operated by the National Association for Public Health Statistics and Information Systems (NAPHSIS); and
- Department of State systems for verifying data from U.S. Passports, Consular Reports of Birth, and Certifications of Reports of Birth.

Many state DMVs already access one or more of these databases as part of their current licensing process; however, the fact that this data verification will now be done by fifty-six jurisdictions – the fifty states plus the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands -- heightens privacy concerns about how the data checks will be performed, who will administer and operate the state query of federal reference databases, how the query or queries will be structured, who will have access to the data, and what will be the business rules surrounding the check to protect the privacy of the applicants' data. The NPRM addresses many of these issues by leaving the control and operation of this data check, including the development of the business rules, to the states. Additionally, the NPRM proposes that individual states document their business rules for reconciling data quality and formatting issues and urges states to develop best practices and common business rules by means of a collective governance structure.[17]

---

[15] Note that the database connectivity mandated by the REAL ID Act is in addition to the database connectivity/functionality required to implement the Department of Transportation's existing control over commercial driver's licensing. In addition, law enforcement already have access directly to a state's driver history via NLETS, which is the International Justice & Public Safety Information Sharing Network, a message switching system serving the criminal justice community.

[16] The DHS Privacy Office is conducting a Privacy Impact Assessment for the SAVE program. It will be published on its website at www.dhs.gov/privacy.

[17] "Privacy Considerations," Section II.C.1(a) of the NPRM.

A very important example of how administration of the data check will be left to the states is the commitment by DHS in the NPRM to support the development of a "federated querying service" enabling the states access to federal reference databases in a timely, secure, and cost-effective manner.[18] Most states query some of these federal reference databases either directly or indirectly today through a portal provided by the American Association of Motor Vehicle Administrators (AAMVA).[19] DHS indicates in the NPRM its commitment to expediting the development and deployment of a common querying service to facilitate the state DMV queries for REAL ID data verification. Since certain databases will be connected, it will be critical from a privacy perspective to clarify which parties control the data systems and which parties have access to the data systems.

To address the privacy concerns posed by such a federated querying service, the Preamble to the NPRM contains a number of important statements. First, it sets forth the narrow purpose of the service: "The purpose of this federated querying service will be to minimize the impact of data verification on State DMV business processes and reduce the costs of data access."[20] Second the Preamble goes on to make the following commitment: "DHS will support the development of [a] querying service but will not operate or control this service." And third, it states: "A frequently-heard concern relates to the amount of additional information the Federal Government will have about driver's license holders and what the Federal Government will do with that data. In fact, however, neither the Real ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before. Moreover, there is no information about a licensee that the Federal Government will store that it is not already required to store."[21]

The commitments made in the NPRM demonstrate that DHS does not intend to expand the purpose for which the querying service will be built and will seek to mitigate the privacy concerns. In addition, the NPRM states that use of this federated querying service will be voluntary and that states may choose to: maintain or establish direct access to the reference databases; combine direct access with partial use of a common service; or verify applicant data against the reference databases in some other manner. Leaving the control and operation of the licensing verification with the states helps mitigate the fears expressed by some that the REAL ID Act will result in a national database operated by the federal government.

Furthermore, as part of the state certification mandated by Section 202(a)(2) of the REAL ID Act, the NPRM proposes that each state prepare a Comprehensive Security Plan for its DMV facilities and the driver's license information storage and production facilities, databases and systems. (See Proposed Rule § 37.41 and Preamble section II.K.) As part of this, each state will submit a privacy policy regarding the personal information collected and maintained by the DMV and will demonstrate how it will protect the information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents, and standards and procedures for document retention and destruction. Also, the Privacy Considerations section of the NPRM notes that DHS expects that a state's certification should demonstrate

---

[18] "Connectivity to Systems and Databases Required for Verification," section II.E.6 (a)(ii) of the NPRM.

[19] Founded in 1933, AAMVA is a nonprofit voluntary association representing the State and provincial officials in the United States and Canada who administer and enforce the laws that govern motor vehicle operation, the driver credentialing process, and highway safety enforcement. DMV administrators are appointed by their State governors and serve on the AAMVA Board of Directors and its committees. AAMVA has played an integral role in the development, deployment, and monitoring of both the commercial driver's license (CDL) and motor carrier safety programs throughout the United States, and its members are responsible for administering these programs at the State level.

[20] "Privacy Considerations," Section II.E.6 (a)(ii) of the NPRM.

[21] "Privacy Considerations," Section II.C of the NPRM.

that it has implemented best practices to protect the privacy of the license holder as guided by the fair information principles that underlie the federal, state, and international law and codes of practice. (See further discussion of the Comprehensive Security Plan in section II.B of the PIA, below.)

3. The State-to-State Data Exchange

Section 202(d)(12) of the Act mandates that states provide electronic access to information contained in the motor vehicle database of the state to all other states, and Section 202(d)(13) requires that the state motor vehicle database contain, at a minimum, all data fields printed on driver's licenses and identification cards and motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on licenses.[22] (See Proposed Rule § 37.33.) These two provisions mandate a state-to-state data exchange. The NPRM contemplates that the states will work collectively to determine the business process and data access rules necessary to implement these provisions prior to May 11, 2008.[23]

As described in Section II.E of the NPRM, although the REAL ID Act poses a requirement for this state-to-state data exchange, this exchange is already required and implemented under the Department of Transportation's (DOT) existing rules and regulations governing commercial driver's licenses (CDLs).[24] The DOT requires that states connect to the National Driver Register (NDR)/Problem Driver Pointer System (PDPS)[25] and the Commercial Driver's License Information System (CDLIS) in order to exchange information about commercial motor vehicle drivers, traffic convictions, and disqualifications. A state must use both the NDR/PDPS and CDLIS to check a driver's record, and also check CDLIS to make certain that the applicant does not already have a CDL.[26] Under these programs, as well as under the REAL ID Act, the primary purpose of the state-to-state data exchange is to determine if the applicant is unqualified and if the application is fraudulent rather than specifically verifying the applicant's identity.

---

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

[23] *See* the Privacy Considerations section of the NPRM.

[24] Commercial drivers licenses (CDL) are governed by the National Driver Register Act of 1982 and the Commercial Motor Vehicle Safety Act of 1986 (CMVSA), both implemented by DOT. (49 U.S.C 31311(a)) as amended.) The CMVSA requires that a commercial driver license (CDL) holder have one and only one driver license and driver record, meaning that a CDL license holder cannot hold a non-CDL from another jurisdiction. The Commercial Driver's License Information System (CDLIS) was consequently developed to enable the record checks of the nation's professional truck and bus drivers, including drivers of HAZMAT vehicles. It is an enhanced, pointer system that requires the states to update records and exchange data. CDLIS maintains nine data elements on all CDL holders: name and aliases, date of birth, SSN, driver's license number, state of record, gender, height, weight, and eye color. All other information is retained by the licensing state.
When CDLIS was first built, states were required to check CDLIS before issuing a CDL to make sure someone did not have a CDL in a previous state. That requirement was not enough, however, to prevent someone from obtaining a non-CDL license in a different state and using that license when driving his own car. As a result, the DOT's Federal Motor Carrier Safety Administration (FMCSA) developed new regulations under the Motor Carrier Safety Improvement Act (MCSIA) of 1999 to require that ALL license applicants be run against CDLIS to address this loophole. (23 CFR § 1327.5) CDLIS is operated by AAMVA on behalf of DOT and is accessed through AAMVAnet, a network service operated by AAMVA.

[25] The NDR/PDPS was established by the National Driver Register Act of 1982 and is administered by National Highway Transportation Security Administration (NHTSA) but accessed through AAMVAnet.
The PDPS is used to search the NDR and will "point" the inquiring jurisdiction to the State of Record, where an individual's driver status and history information is stored. The NDR contains identification data for individuals under suspension or revocation, and/or who have committed serious motor vehicle-related violations. By compact or convention, every state respects every others state's suspensions/revocations. The PDPS record contains five data elements: name and aliases, date of birth, driver's license number, and State of Record. Jurisdictions have the option of also sending SSN, height, weight, and eye color. The 2003 Privacy Impact Assessment for the NDR is posted at http://www.dot.gov/pia/nhtsa_ndr.htm

[26] A state may also send a query to another state for the full history of a driver without going to the CDLIS or PDPS pointer files. Only certain highway-safety related offenses are transmitted on a driver's history obtained from PDPS.

The existing state-to-state data exchange among DMVs, while focused on commercial driver's licensing, also impacts non-commercial license applicants, as states are required currently to run all license applicants against the PDPS and CDLIS, which are both pointer systems that collect limited information from each state in order to match against the incoming inquiries. Both systems offer certain mandatory privacy protections.

The PDPS is subject to federal regulations 23 CFR Sections 1327.1 et seq., which adopts the Privacy Act of 1974[27] principles of individual participation and collection, use, and disclosure limitation. On the other hand, CDLIS may be subject to more limited privacy protections, because DOT's policy states that CDLIS is not a federal "system of records," as defined by the Privacy Act since the records in CDLIS are not controlled by DOT's Federal Motor Carrier Safety Administration (FMCSA).[28] Under DOT policy, drivers who wish to review and, if necessary, correct information about them in CDLIS must contact the state agency that issued their license. Access to CDLIS is limited to DOT, the states, an employer or prospective employer of a person who operates a commercial motor vehicle, and to federal agencies upon written request where there is a legal basis and need.[29] DHS is not aware of any privacy issues with the CDLIS implementation.

The NPRM states that DHS intends to work closely with the DOT, AAMVA, and the states to fulfill the requirements for the state-to-state data exchange under the REAL ID Act, while also supporting privacy protections for this exchange. It has not been determined whether CDLIS or some other service will be the platform for the state-to-state exchange, but regardless of the platform, it will be necessary for the states, working with DHS and DOT, to define the privacy protections for any state-to-state data exchange, including how it will be operated and controlled and who will have access.

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

B. How will personal information required by the REAL ID Act be protected in the state databases?

At the federal level, only the Driver's Privacy Protection Act of 1994 (DPPA)[30] addresses the privacy of motor vehicle records, but its protections are narrowly focused. The DPPA addresses the use and disclosure of personal information stored in state motor vehicle records, but it does not prescribe privacy protections for the personal information stored on the credentials themselves nor does it set any security requirements for the motor vehicle databases. Rather, the DPPA simply prohibits DMVs from disclosing "personal

[27] The Privacy Act of 1974, 5 U.S.C. §552a.
[28] FMCSA's Policy on Availability of Information From the Commercial Driver's License Information System, 70 Fed. Reg. 2454, January 13, 2005.
[29] Id. A federal agency is required to execute a Memorandum of Understanding with DOT and/or FMCSA before access to CDLIS data will be provided.
[30] Pub. L. 103-322 as amended by Pub. L. 106-69, 18 U.S.C. § 2721 et seq.

information" contained in a DMV "motor vehicle record,"[31] unless the disclosure falls within fourteen permissible uses,[32] including disclosure to any federal, state or local government agency to carry out that agency's legitimate functions. In effect, the DPPA serves only as a prohibition on the sale of the personal information found in motor vehicle records for marketing purposes.[33] Consequently, the personal information found in motor vehicle records is widely available through information brokers for the enumerated uses including fraud prevention and insurance purposes. Moreover, the DPPA authorizes resale or redisclosure of the information so long as it is for one of the fourteen permissible uses, making abuses of the DPPA very difficult to monitor or, even, to trace.[34] Therefore, DHS cannot rely on the DPPA to protect the privacy of the personal information required under the REAL ID Act.

Section 202(d)(7) of the REAL ID Act requires states to "ensure the physical security of locations where driver's licenses and identification cards are produced and the security of document materials and papers from which driver's licenses and identification cards are produced." The NPRM relies on this provision as authority for DHS to define basic security program requirements to ensure the integrity of the REAL ID driver's licenses and identification cards and to protect the security of the personal information stored in DMV databases associated with these driver's licenses and identification cards.[35] The NPRM notes that the House Conference Report discussion of this section of the Act expressed concern with the "growing problem of identity thieves and document purveyors breaking into state facilities and stealing driver's license or identification card stock blanks, printing machines, and sometimes actual computer hard drives in which current driver's license or identification card holder data is stored."[36] Also the NPRM cites to the number of state DMVs that experienced incidents of theft of personal information from their databases[37]

---

[31] The DPPA authorizes 14 permissible uses for "personal information," which it defines to include "an individual's photograph, social security number, driver identification number, name, address (except the five-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3). It defines a "motor vehicle record" as "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1).

[32] The permissible uses are: (1) use by any government agency, including any court or law enforcement agency, in carrying out its functions; (2) use in connection with motor vehicle-related matters (motor vehicle or driver safety and theft; motor vehicle emissions, motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, parts and dealers by motor vehicle manufacturers, motor vehicle market research activities, and removal of non-owner records from the original owner records of motor vehicle manufacturers); (3) use in the normal course of business by legitimate businesses, but only to verify accuracy of personal information submitted by an individual to the business and if no longer correct to obtain correct information but only for purposes of preventing fraud by pursuing legal remedies against or recovering on a debt or security interest against the individual; (4) use in connection with a civil, criminal, administrative, or arbitral proceeding; (5) use in research activities so long as the personal information is not published, redisclosed, or used to contact individuals; (6) for use by any insurer; (7) use in providing notice to the owners of towed or impounded vehicles; (8) use by any licensed private investigative agency for a permissible purpose; (9) use by an employer or its agent or insurer to obtain or verify information of a holder of a commercial driver's license; (10) use in connection with operation of private toll transportation facilities; (11) any other use in response to requests for a record if the State has obtained express consent of the person; (12) for bulk distribution of surveys, marketing or solicitations if the State has express consent of the person,; (13) use by any requester, if the requester demonstrates it has obtained written consent of the individual; and (14) for any other use specifically authorized under the law of the State holder of the record, if such used is related to the operation of a motor vehicle or public safety.

[33] Originally the DPPA permitted sale of record information for use in marketing activities if the individual was given an opportunity to opt out. In 1999, Congress amended the law to require that DMVs obtain express consent for sale of record information for marketing purposes.

[34] 18 U.S.C. § 2721(c)

[35] *See* discussion in NPRM Preamble Sections II.K.4 and 5 and Proposed Rule § 37.41.

[36] H.R. Rep. 109-72, at 183 (2005) (Conf. Rep.).

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

and that federal and state governmental agencies have made security of personal information a high priority.[38]

Specifically, the NPRM proposes that each state submit, as part of the REAL ID Act certification process, a written document to be known as the Comprehensive Security Plan. This certification requirement provides an important safeguard for the personal information collected, used, and maintained by state motor vehicles offices and assures the public that the state handles personal information appropriately. As part of the Comprehensive Security Plan, states will provide a privacy policy;[39] describe "reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the physical location and the personal information stored and maintained in DMV records and information systems";[40] and describe the state's "standards and procedures for safeguarding information collected, stored or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction."[41] In addition, Section II.K.5 of the NPRM encourages states to draft collective standards and best practices for the management of both documents and data proposed under the provisions of the rule.

The NPRM proposal for the Comprehensive Security Plan provides an important privacy protection, because the Plan will assist the states to address most, if not all, of the Privacy Office Fair Information Principles as described at the outset of this PIA. The Privacy Considerations section of the Preamble to the NPRM states that the plan "should demonstrate that it has implemented best practices to protect the privacy of the license holder as guided by the fair information principles, which call for openness, individual participation (access, correction, and redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing, and that these principles are widely recognized and embodied in numerous federal, state, and international law and codes of practice."[42] DHS is requesting comments on recommended best practices for protecting the privacy of the personal information stored in the various state motor vehicle databases pertaining to the requirements under the REAL ID Act. The Privacy Office supports appropriate privacy protections and procedures to protect the personal information associated with implementation of the Act that are consistent to the greatest extent possible with the Fair Information Principles.

C. How will the personal information stored on the machine readable technology on the licenses and IDs be protected from unauthorized collection and use?

The implementation of any digitized collection of information increases the efficiency by which that information can be accessed. Records, which were once accessible only in human-readable format, in digital form can be readily accessed and then used in ways beyond the original purpose of the records. This inherent capacity of digital records requires closer scrutiny of which records and what information is accessible in digital form, because efficiency in access and availability for additional uses raises important privacy issues.

---

[38] *See* Office of Management and Budget Memoranda, M-06-15, M-06-16, and M-06-19.
[39] Proposed Rule § 37.41(b)(5)
[40] Proposed Rule § 37.41(b)(1)(iii)
[41] Proposed Rule § 37.41 (b)(8)
[42] *See* NPRM section II.C.2.

Sections II.H.7-9 of the NPRM review the issues surrounding the personal information stored on the machine readable technology (MRT) on the REAL ID licenses and IDs. The REAL ID Act standardizes the minimum personal information on the ID and mandates the use of a MRT. The NPRM proposes that states use the PDF-417 2D bar code and indicates that DHS leans toward recommending that states protect the personal information stored in this 2D bar code by requiring encryption, if the operational complexity of deploying a nationwide encryption infrastructure to provide access to law enforcement can be addressed. The issue of encryption of the 2D bar code is one of software and infrastructure costs and not hardware cost, since the widely used 2D bar code reader can also be used to read the encrypted data.

The NPRM discusses the privacy concerns raised by the potential for unauthorized third parties to collect and use the personal information on REAL ID driver's licenses and identification cards via a machine readable zone (MRZ). Although DHS lacks authority to prohibit third-party access to the information in the MRZ, DHS can determine to require technological protections to the MRZ, because the REAL ID Act gives DHS authority to select the technology and its implementation.

As discussed earlier in this PIA, the DPPA has not been interpreted to provide any privacy protections for the personal information stored on the driver's licenses. Currently, most states use the 2D bar code recommended in the NPRM, exposing the information stored on the credential to unauthorized collection or "skimming," the term often used to describe this sort of information capture by unauthorized third parties. Readers for the 2D bar code are readily available for purchase on the Internet and at a very low cost, which permits unauthorized third parties to skim the information for their own business needs or to sell to other third parties.

With skimming an existing problem, the REAL ID Act does not contain any statutory language to address the downloading, access, and storage by third parties of the information in the MRZ. Third parties, such as retailers, hotels, bars, and convenience stores, could invest in economical skimming devices to access information on any individual's credential for unauthorized uses. Furthermore, the Act's requirement that each REAL ID credential contain a unique identifier provides an opportunity for third parties to normalize data stored about individuals within large data warehouses. Like the situation with SSNs, this normalization would provide links between the identifier and the individual. Thus, if a retail entity were to collect just the unique identifier from the REAL ID credential and associate it with the transactional information related to the interactions the individual has with the retailer, this information could be useful to any third party. The REAL ID Act presents two risks in this situation. One, greater amounts of data about transactions could be linked to an individual. Two, third parties may assume that the credential holder was in fact the credential owner and so may not verify sufficiently the picture and/or signature on the credential, as often occurs today with credit cards. This could lead to the possibility of incorrect information being linked to an individual because of an incorrect recording of the unique identifier.

As usual, individuals will likely be unaware that their personal information on the credential has been retained by the third party, since individuals assume the third party to whom they gave the ID merely checked the information against a database for a valid purpose, such as validating an individual's age. Moreover, when a third party appropriates the personal information, individuals are often unaware, and therefore do not associate the use of their ID with unsolicited marketing or identity theft or fraud.

1. Statutory Protections

A few states have laws that expressly protect the privacy and security of the personal information encoded on driver's licenses and identification cards. For example, California,[43] Nebraska,[44] New Hampshire,[45] and Texas[46] have enacted laws to limit the skimming of driver's license or identification card information. In addition, AAMVA has drafted a "Model Act to Prohibit the Capture and Storage of Personal Information Obtained from a Driver's License or Identification Card," which allows third party users to use a transaction scan device, like a 2D bar code scanner, on the driver's license or identification card for the limited purpose of age verification. The Model Act, which prohibits any other non-governmental use of the information without the express written consent of the card holder,[47] would provide legal authorities creating privacy protections. The Privacy Office strongly encourages that all 56 jurisdictions consider and enact laws that expressly protect the privacy and security of information contained on their driver's licenses and identification cards, because this will also help address the growth of the unique REAL ID identification number becoming a *de facto* national ID by limiting its uses.

2. Ensuring Law Enforcement Access

Nonetheless, as described above in the Legislative History section of this PIA, the House Conference Report states that the overall purpose of Section 202(b)(1) is to "improve the ability of law enforcement officers at all levels to confirm the identity of the individuals presenting state issued driver's licenses or identification cards." The House Conference Report recognizes that financial institutions and even retail establishments may wish to use the credential to verify an individual; however, the Report indicates that such verification would be done using the person's signature on the credential and not the MRZ. (See House Conference Report discussion of Section 202(b)(7)) regarding the requirement for a signature.) Neither the Act nor the House Conference Report support harvesting the information from the MRZ on the credentials.

For these reasons, to the extent permitted under the Act, the use of the personal information on the REAL ID credentials should be limited to identity verification and law enforcement purposes.[48] Although there is no language in the REAL ID Act that limits how retailers, bars, banks or other third parties may use the personal information on the REAL ID driver's licenses or identification cards, the NPRM invites comment

---

[43] Confidentiality of Driver's License Information, California Civil Code 1798.90.1 (Effective January 1, 2004).

[44] Storage or Compilation of Information, Revised Statutes of Nebraska 60-4,111.01 (2001). The Nebraska law limits storage or compilation of information from the license or State identification card to the statutorily authorized purposes of the DMV, the courts, or law enforcement agencies. Violation of the law is a felony.

[45] Drivers' Licenses Prohibitions, New Hampshire Revised Statutes, Title XXI, Motor Vehicles, Chapter 263, Section 263:12 (Effective January 1, 2003). The law prohibits scanning, recording, or storing of the personal obtained from the license unless authorized by the department. Non-electronic transfer of the information on the face of the license is prohibited without the consent of the license holder, except to law enforcement.

[46] Electronically Readable Information, Texas Statutes, Transportation Code, Title 7 Vehicles and Traffic, Chapter 521 Driver's Licenses and Certificates, Section 521.126 (Effective September 1, 2005). The law limits access to law enforcement, to identify a voter, to financial institutions for identification purposes and only with express consent, and upon authorization of a maritime facility to secure the facility or port.

[47] AAMVA 26-8.2-03, 2003. If the commercial user has a reasonable basis to believe that the identification card has been tampered with, or has been fraudulently issued or produced, the user may record and maintain the encoded information but only for the purpose of reporting it to appropriate administrative or law enforcement officials.

[48] Although businesses and non-governmental entities may use the credentials for the purpose of identity verification, express prohibitions from collecting and storing the information help mitigate privacy risks. Retailers and financial institutions can continue to examine the name, signature, and photo on the credentials for purposes of identity verification and the date of birth to verify age.

on ways to enable law enforcement officials to have access, while limiting access to unauthorized third parties for inappropriate uses.

3. Technological Protections

Further, in order to address both privacy issues and law enforcement needs, the NPRM asks for comments on means and methods to limit unauthorized third parties access to the digital information[49] on the credential. As noted above, the mandatory data elements to be included within the bar code are, as proposed by the NPRM: expiration date, holder's name, issue 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 ID), and the inventory control number of the physical document. Because 2D bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential. For example, a bar that required a license could quickly scan the 2D bar code to prove that a person was 21 or over to enter the bar, but at the same time conceivably obtain the person's name and address and compile a list of names and addresses of its patrons, along with the other encoded data, including the unique identification number, which the bar could subsequently sell or use.

Encryption can help mitigate this privacy risk because it would prevent the downloading of the information on the MRZ into a database. Of course the encoded data remains available and accessible on the face of the card in human-readable form; however, encryption lessens the likelihood of the collection, because it would reduce the efficiency of the digital information on the credential by limiting access to only those parties, such as law enforcement, that require the information, but retains efficiency for parties permitted to access the information. Even if a third party compromises or breaks the encryption, which would be difficult, the encryption would still protect against most skimming, as most third parties would not have access to the compromised key. Further, at that point, the cryptographic key could be modified to protect credentials issued after the compromise of the encryption.

Because encryption of the data necessitates access to the cryptographic key required to decrypt the data, employing encryption in the 2D bar code would require having a key infrastructure allowing permitted parties access to the secured key information. The need for a key infrastructure to support access to encrypted 2D bar code data raises an important challenge for implementation of encryption.

In the NPRM, DHS asks for comment to determine (1) if implementing encryption is feasible from an operational and cost perspective and (2) if encryption can be deployed in a manner ensuring access to the information by law enforcement. It is recognized that implementing encryption would likely require a complex and comprehensive exchange of encryption keys among all fifty-six jurisdictions involved in issuing and accessing REAL ID driver's licenses and identification cards. Building such an infrastructure would have certain complexities that, if not addressed appropriately, could reduce the utility of creating such standards for encoding data into the 2D bar code.[50]

---

[49] For the machine-readable portion of the card, the proposed machine-readable technology standard is the PDF-417 2D bar code, although a State may use any other technology in addition to a PDF-417 bar code as long as the driver's license or identification card complies with the PDF-417 2D bar code standard.

[50] With 2D bar codes, a symmetric cryptographic key system would need to be implemented. With a symmetric system, a multi-key or single key implementation could be used. In a multi-key implementation, although a larger the number of keys creates a more secure the system, because a single key compromise does not compromise the entire system, this large number of cryptographic keys would need to be accessible to the law enforcement personnel wherever they would be reading the driver's

Encryption is increasingly being used in the private sector to protect against unlawful access and possible identity theft. In the public sector, encryption will be used to protect the personal information stored on the HSPD 12 federal identification cards as well as on the DHS Transportation Workers Identification Credential (TWIC) IDs. While there are costs to encryption, the DHS Privacy Office believes the benefits of protecting the personal information could outweigh these costs, if it is feasible to use encryption within the necessary operational context.

4. Data Minimization Protections

The NPRM mandates that the bar code include a significant number of data elements: the expiration date, holder's name, issue 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 ID), and the inventory control number of the physical document. If the operational and cost hurdles of implementing encryption prove too high, DHS could request states to leave the proposed federally-required elements unencrypted, while permitting encryption of only the "state-specific" elements. For example, if a state wished to include a digital photograph in the MRZ, it would be free to do so and encrypt it, as the photograph is not currently one of the mandatory REAL ID data elements. Another option would be for DHS to omit the address information from the MRZ, making skimming less attractive to third parties. In this regard, the NPRM seeks comments on whether a demonstrable law enforcement need exists to include the address on the MRZ portion of the REAL ID driver's license, such that address should be included as a mandatory data element on the MRZ. One specific option to preventing not only the efficient use of the skimmed information, but also preventing the establishment of a national ID, would be not to place the unique identification number in the MRZ. The number could still be on the face of the credential for use by law enforcement, but not including it in the MRZ may lessen its attractiveness for collection by unauthorized parties. These options would limit the type and amount of information available in digital form.

Further, if it is determined that the data elements cannot be encrypted, it will be critical to inform driver's license and identification card holders about their need to monitor carefully the handling of the REAL ID credentials when physically providing them to third parties. The more sensitive the personal information elements maintained on the REAL ID credential, the more likely unauthorized third parties will target this information to engage in data aggregation, marketing, fraud, theft, or other illegal activities.

Good privacy policy supports limiting the data in the MRZ to the minimum personal data elements necessary for the intended purpose of providing access to law enforcement personnel. This minimizes but does not eliminate the opportunity for unauthorized third parties to use personal information for unrelated, secondary purposes. Thus an unencrypted MRZ should have fewer data elements and more limited personal information, especially the credential holder's address. In its discussion of section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," the House Conference Report clearly indicates that Congress wanted to address privacy by minimizing

---

license. A single key implementation would avoid the complexities of needing a key infrastructure, but this greatly increases the risk that this single key could be compromised. Although employing a single key greatly simplifies the procedure to make available the cryptographic key to law enforcement personnel, the compromise of this single cryptographic key would compromise all driver's licenses created with it. In this case, encryption could create a false sense of security if a license holder thought his or her information was truly secure and it was not, because an unauthorized third party compromised the key. Not only do these implementation operations present operational and security risks, they also factor into the privacy risks with the selection of an implementation.

exposure of the information: "There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with *other data stored securely and only able to be read by law enforcement officials*."[51] This statement suggests that Congress wanted to secure the privacy of the data contained on the MRT and make it accessible only to law enforcement officials. The only way currently available to control access to the data on the MRT is to encrypt it. Strong privacy and security concerns exist regarding the selection of a MRT because, if not done right, the MRT could facilitate identity theft and unauthorized collection of the personal information on the REAL ID credential. Therefore, encryption standards can control and limit who has access to the information encoded in the 2D bar code in the MRZ to prevent unauthorized parties from harvesting the information and reselling it.

Lastly, to reiterate an earlier point, the DHS Privacy Office is hopeful that the states will take action similar to that of California, Nebraska, New Hampshire, and Texas to prohibit non-governmental entities and individuals from harvesting the information on driver's licenses or identification cards for any purpose whatsoever. Retailers and financial institutions should be able to continue to examine the Real IDs for purposes of identity and age verification, but should be barred from downloading the information from the machine-readable zone.

D. How do the requirements for a photograph and address on the ID and the DMV employee background check impact privacy?

1. Requirement for a Photograph on the REAL ID

Section 202(b)(5) of the Act requires that the state-issued REAL ID driver's license or identification card include a digital photograph of the individual. In addition, Section 202(d)(3) provides that the state shall require that each individual applying for a driver's license or identification card be subject to mandatory facial image capture.[52] These provisions form the basis for the photograph requirements set forth in Proposed Rule § 37.11(a). This statutory requirement applies whether or not the person ultimately receives a driver's license or identification card, since the Act refers to "each person applying" for a driver's license or identification card. If a driver's license or identification card is not issued, the NPRM proposes that states dispose of the photograph after one (1) year. In addition, the NPRM proposes that DMVs update the photograph in the event the applicant reapplies and to discard prior photos. If the DMV does not issue the driver's license or identification card because of suspected fraud, the DMV would be required to maintain the record for ten (10) years and reflect that a driver's license or identification card was not issued for that purpose.[53]

The NPRM acknowledges that some individuals who apply for a REAL ID driver's license or identification card may oppose having their photograph taken based on their religious beliefs;[54] however, the REAL ID Act requires a facial photograph to enhance security. DHS therefore has no option other than to propose

---

[51] Italics for emphasis, not in the original. H.R. Rep. 109-72, at 179.
[52] DHS is proposing that digital photographs comply with current ICAO standard 9303 Part 1 Vol. 2, specifically ISO/IEC 19794-5 - Information technology - Biometric data interchange formats - Part 5: Face image data, which is incorporated into ICAO 9303. This calls for a full face image from the crown to the base of the chin and from ear-to-ear (unless the State chooses to use profiles for licensees under 21), and images with no veils, scarves or headdresses to obscure facial features, or eyewear that obscures the iris or pupil of the eyes.
[53] *See* Proposed Rule § 37.11(a)
[54] *See* NPRM section II.H.3.

that states that issue non-photo driver's licenses or identification cards based on an individual's religious beliefs do so as long as those driver's licenses or identification cards are issued in accordance with the rules for non-compliant driver's licenses and identification cards.

Prior to issuing the NPRM, the DHS Office of Civil Rights and Civil Liberties facilitated a meeting with civil rights and citizen representatives at which DHS staff heard specifically about the concerns of the Amish and Muslim faith with regard to requiring a photograph on a REAL ID Act credential. These groups argued that the Religious Freedom Restoration Act (RFRA), 42 U.S.C. § 2000bb-1, states that "Government shall not substantially burden a person's exercise of religion even if the burden results from a rule of general applicability" unless the application of the burden "is in furtherance of a compelling governmental interest" and "is the least restrictive means of furthering that compelling government interest." Since the REAL ID Act mandates the photograph, DHS has no flexibility to address the legitimate concerns of such groups, other than to permit states to provide individuals with non-photo driver's license and identification card as long as the states issue such credentials in accordance with the rules for non-compliant driver's licenses and identification cards.

2. Requirement for Address of Principal Residence

Section 202(b)(6) of the Act requires that the driver's license or identification card include the individual's address of principal residence. The NPRM proposes to exempt certain individuals from this requirement consistent with (1) existing state laws and current exceptions processes by states to protect victims of domestic violence, judges, protected witnesses, and law enforcement personnel, and (2) Section 827 of the Violence Against Women and Department of Justice Reauthorization Act of 2005,[55] which amended the REAL ID Act 2005 (49 U.S.C. 30301 note) to protect against disclosure of addresses of individuals who have been subjected to battery, extreme cruelty, domestic violence, dating violence, sexual assault, stalking, or trafficking. Consequently, the NPRM proposes to exempt the following from the address requirement: (1) an individual enrolled in a state address confidentiality program; (2) an individual who's address is entitled to be suppressed under state or federal law or suppressed by a court order; or (3) an individual protected from disclosure of information pursuant to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

Most states retain the "actual" address in their database, but often protect it so that only authorized personnel have access to the "actual" address. In addition, most states do not have the "actual" address in the MRZ on the credential. Rather, the MRZ contains only what is on the face of the driver's license or identification card. Therefore, the NPRM proposes to exempt individuals who are entitled to enroll in state address confidentiality programs, whose addresses are entitled to be suppressed under state or federal law or by a court order, or who are protected from disclosure of information pursuant to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 from the requirement to have their address displayed on REAL ID driver's licenses and identification cards. The NPRM also notes that other categories of individuals, such as federal judges, may also require that their addresses remain confidential to protect their safety and invites comment on how these categories of individuals can be protected, while remaining consistent with requirements of the Act.

[55] Title VIII, Subtitle C, Sec. 827 (Pub. L. 109-162, 119 Stat. 2960, 3066, Jan. 5, 2006)(Protection of domestic violence and crime victims from certain disclosures of information).

In addition, the NPRM acknowledges that some people do not have a fixed address and that states have exceptions processes in place to address this situation. For example, in some states homeless people may use addresses of accredited organizations. The NPRM provides a mechanism by which states may continue to address these situations through a written and documented exceptions process. Exceptions processing is referenced in Proposed Rule § 37.11(h) and discussed further in section II.F of the NPRM.

The approach provided in the NPRM addresses the legitimate privacy concerns associated with disclosing addresses of these individuals. The Privacy Office believes the disclosure of addresses in the MRZ of all other REAL ID driver's license and identification card holders is better addressed by encryption as discussed above in Section II.C of the PIA.

3. Requirement for DMV Employee Background Check

Section 202(d)(8) of the REAL ID Act requires that "all persons authorized to manufacture or produce driver's licenses and identification cards" must be required to undergo "appropriate security clearance requirements." Proposed Rule § 37.45 addresses the requirements of Section 202(d)(8) of the Act by identifying which categories of DMV employees must undergo "background checks"[56] and the nature of the background checks. The NPRM discussion of the mandated background check states that Congress made it clear that Section 202(d)(8) was intended to address cases of insider corruption,[57] and therefore, the NPRM proposes that background checks be required for "DMV employees or DMV contractors who have the ability to affect the recording of any information required to be verified, or who are involved in the manufacture or production of driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card."[58]

The NPRM recognizes that each state's DMV has a unique organization and structure, and leaves it to each state to identify the "covered positions" that would fall under this definition. Also, the NPRM proposes that the state DMVs provide employees and prospective employees selected for placement in a covered position with notice that a background check is required for employment in a covered position and what that background check will include. Such notice is consistent with federal Privacy Act notice requirements.[59]

With respect to the type of background check required, the NPRM proposes that states collect fingerprints for individuals who seek employment in a covered position, in order to conduct a "criminal history record check" (CHRC) on those individuals through the Federal Bureau of Investigation (FBI) and state repositories. It also specifies a list of disqualifying offenses, based on current federal requirements, that mirrors requirements for DHS Transportation Security Administration's Hazardous Materials Endorsement program (HAZMAT program) and Transportation Workers Identification Credential (TWIC) program.[60]

---

[56] The NPRM defines a background check as an investigation into someone's past history to permit them to either gain a security clearance or pass a suitability screening. It notes that a security clearance is the end result of a background investigation whereby the government makes a determination that someone may be trusted with specified levels of information, such as "classified" information. While section 202(d)(8) of the Act uses the term "security clearance," DHS concludes that the intent was to conduct background checks, as DMV employees do not need clearance to handle "classified" information.
[57] H.R. Rep. at 183.
[58] *See* definition of "covered employees" in the Proposed Rule Definition § 37.03 and the discussion of this provision in NPRM Section II.K.1.
[59] *See* 5 U.S.C. § 552a(e)(3).
[60] *See* 49 CFR 1572.103 and the final rule on TWIC (72 Fed. Reg. 3492 (Jan. 25, 2007).
Section 37.45 of the NPRM defines the offenses as follows:

The NPRM states that this list of crimes is sufficient as a federal minimum; but that states may add additional disqualifying offenses to this list for their covered employees and invites comment on whether the proposed list of disqualifying offenses is appropriate, too large, or insufficient as it concerns REAL ID.

In addition to the criminal history record check, the NPRM proposes that states perform a "financial history check" on individuals seeking employment in covered positions in a manner consistent with the Fair Credit Reporting Act. Although a number of states already collect fingerprints of their employees and run criminal history record checks, it is not clear how many currently perform financial history checks. Although many employers, including many DMVs, already conduct financial history checks as one indicator that an individual may warrant additional scrutiny or supervision before assuming responsibilities that raise security risks, concerns exist about how such a check may be applied by the states under this regulation. The NPRM states that while questionable financial history would not be considered a federal disqualifier, the information should be used by the states in making their own determinations on how or whether particular individuals should be employed at the DMV.

The NPRM acknowledges that the proposed requirement for a financial history check is not a feature of the TWIC or HAZMAT programs, but states that DHS believes that it is warranted in this case, due to the sensitivity of the personal information that will routinely be handled by employees at state DMVs and the fact that a driver's license or identification card serves as a key source document in securing other forms of state and federal identification. The NPRM persuasively states that "[i]f the DMV personnel issuing and authenticating the driver's license or identification card are compromised and issue genuine REAL ID driver's licenses and identification cards to individuals who are seeking to mask their true identity, those individuals can obtain additional identification using that false identity and thwart the Government's and law enforcement's ability to identify accurately individuals lawfully stopped and screened."

Employees who are susceptible to corruption should not be hired for covered positions, but it will be critical that DMVs assess the financial history information fairly and take extenuating circumstances into consideration when making this determination. It is not clear what financial difficulties a state would use to disqualify an individual from employment.

Although the NPRM does not propose to preclude a DMV from hiring any individual based on the results of the financial history check and does not propose to preclude the DMV from placing the individual in a covered position based on that check, because financial history records can include inaccurate or out-dated information, it is not clear that DMVs will be able to evaluate the information appropriately. From a privacy and security perspective, the criminal background check provides the best understood indication of whether or not an employee may pose a security risk. Importantly, the NPRM states that individuals denied

---

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

(ii) Interim disqualifying criminal offenses. The criminal offenses referenced in 49 CFR 1572.103(b) are disqualifying, if the applicant was either convicted of those offenses in a civilian or military jurisdiction, or admits having committed acts which constitute the essential elements of any of those criminal offenses within the seven years preceding the date of application; or the applicant was released from incarceration for the crime within the five years preceding the date of application.

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

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

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

employment based on the background check must be given notice and an opportunity to appeal to the state.

The NPRM also proposes that states conduct a lawful status check on covered employees through the Systematic Alien Verification for Entitlements (SAVE) program run by DHS U.S. Citizenship and Immigration Services (USCIS) to verify that the individual has lawful status in the United States.

States may grant waivers allowing individuals to maintain their positions under particular circumstances as authorized by the states, for example, where an individual has made full disclosure of his or her criminal history to the state DMV. Appeals based on the lawful status check will be appealed to DHS.

III. Conclusion

The REAL ID Act implicates a number of significant privacy concerns for the American public. This PIA seeks to identify the concerns and describe how the Department's NPRM has addressed them. In the key areas, the NPRM proposes important privacy protections in furtherance of the authority provided to DHS under the REAL ID Act and further clarification in the final rule will ensure their implementation and enforceability. These privacy protections should include: (1) providing for state control and operation of the state query of federal reference databases and the state-to-state data exchange; (2) requiring states to submit a Comprehensive Security Plan, including a privacy policy and plan to protect the personal information associated with implementation of the Act; and (3) employing encryption to protect the personal information stored on REAL ID driver's licenses and identification cards, while ensuring appropriate law enforcement access.

These protections serve as a floor and do not prevent the states from using their own statutory or executive authority to provide additional privacy protections for the personal information stored on the REAL ID credentials and in the state databases. The Privacy Office believes that protecting the privacy of the personal information associated with implementation of the REAL ID Act is critical to maintaining the public trust that government can provide basic services to its citizens and residents while preserving their privacy. The public is encouraged to comment on the NPRM and on the privacy issues associated with implementation of the Act in order to ensure that the final rule reflects robust public input on these important issues.

Rulemaking Contact

Darrell Williams, REAL ID Program Office, Department of Homeland Security, Washington, DC 20528 (202) 282-9829

Reviewing Official

Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, (571) 227-3813.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security