Privacy Impact Assessment
for the

REAL ID Final Rule

January 11, 2008

Rulemaking Contact Point
Darrell Williams
Director, REAL ID Program Office
DHS Policy Office
(202) 282-9829

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) is issuing a final rule establishing minimum standards for State-issued driver's licenses and identification cards that Federal agencies will accept for official purposes after May 11, 2008, in accordance with the REAL ID Act of 2005, Pub. L. 109-13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note) (the Act). The final rule establishes standards to meet the minimum requirements of the Act including: information and security features that must be incorporated into each card; application information to establish the identity and lawful status of an applicant before a card can be issued; and physical security standards for locations issuing driver's licenses and identification cards.

This Privacy Impact Assessment (PIA) updates the PIA issued on March 1, 2007, in conjunction with the Notice of Proposed Rulemaking (NPRM). (The NPRM and its PIA are posted at www.dhs.gov/privacy.) DHS received over 21,000 comments on the NPRM, including comments on the PIA or privacy issues related to the NPRM. The DHS Data Privacy and Integrity Advisory Committee separately submitted to the DHS Chief Privacy Officer a recommendation on the privacy implications of the requirements proposed in the NPRM. The final rule summarizes the comments and provides brief responses outlining the Department's decisions. This PIA does not duplicate the comment summaries or responses but rather highlights how the final rule addresses the privacy issues outlined in the NPRM PIA. In addition, the "Privacy Considerations" section of the final rule (IV.D.) provides a general response to each of the areas noted in the NPRM PIA.

The DHS Privacy Office is updating the March PIA under the authority of Subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which calls for the DHS Chief Privacy Officer to conduct a "privacy impact assessment of proposed rules of the Department." The PIA analysis reflects the framework of the Privacy Office's Fair Information Practice Principles (FIPPs): Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. In addition, the DHS Privacy Office is releasing its *Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the Real ID Act* (*Best Practices for Protection of PII*) (Attachment A) to provide guidance to State DMVs on privacy and security protections consistent with the FIPPs standards and practices equivalent to those required under the Privacy Act of 1974 (5 U.S.C. § 552a), the Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3542), and the information security standards issued by the National Institute of Standards and Technology (NIST).

Introduction

Under the REAL ID Act of 2005, Federal agencies are prohibited, effective May 11, 2008, from accepting a State-issued driver's license or personal identification card for an "official purpose" unless the issuing State meets the requirements of the Act.[1] "Official purpose" is defined under § 201 of the Act and § 37.03 of the rule to include access to Federal

[1] States requesting a timely extension from DHS may continue to have their existing driver's licenses and identification cards accepted for official purposes even after May 11, 2008. See the final rule for further details.

facilities, boarding Federally-regulated commercial aircraft, entry into nuclear power plants, and such other purposes as established by the Secretary of Homeland Security.

The NPRM PIA analyzed five major privacy areas posed by the Act and the proposed rule: (1) whether the Act and the implementing regulations will result in the creation of a national identity card or database; (2) whether and how the personal information associated with implementation of the Act will be protected from unauthorized access or use; (3) whether and how the personal information stored in the machine readable zone (MRZ) on the cards will be protected against unauthorized use; (4) the proposed requirement that a photograph and address appear on the credential; and (5) the proposed requirement that DMVs conduct a financial history check on covered employees. These issues are addressed below within the framework of the fair information practice principles.

The Privacy Office recognizes that the REAL ID Act poses privacy challenges, particularly in light of the complex and distinct roles of DHS, the Department of Transportation, and the States. The States will continue to issue all driver's licenses in the United States. Congress, through the REAL ID Act, has mandated minimum standards for licenses that can be accepted by Federal agencies for official purposes. DHS will monitor State compliance with those standards. The Act calls for DHS to set certain requirements; however, it is the States that will collect, store, and maintain the personally identifiable information (PII) required for implementing the DHS requirements.

The final rule has sought to address privacy concerns to the extent of DHS' authority. For example, § 37.33(b) of the final rule calls for the security of PII collected pursuant to the Act and § 37.41 calls for States to develop a security plan. In addition, in response to comments, the final rule has eliminated the financial history check for covered DMV employees, which was a proposed requirement in the NPRM.

In conjunction with the final rule and this PIA, the Privacy Office is issuing its *Best Practices for Protection of PII* to provide guidance to State DMVs on privacy and security protections consistent with standards and practices equivalent to those required under the Privacy Act of 1974 (5 U.S.C. § 552a), FISMA (44 U.S.C. § 3542), and the information security standards developed by NIST, including those required for Federal information systems, including the Federal Information Processing Standards Publication 200 (FIPS PUB 200) and the NIST Recommended Security Controls for Federal Information Systems (NIST 800-53). (See PIA Attachment A.) These practices are consistent with other Federal and State laws that implement the FIPPs and are intended to supplement the limited protections of the Driver's Privacy Protection Act (DPPA), 18 U.S.C. §2721 *et. seq*. If implemented by State DMVs, these best practices would contribute significantly to the protection of PII and the public's privacy. In addition, many States have privacy laws that will help ensure that State DMV records and information will be protected from unauthorized uses. The Privacy Office encourages the States to exercise full authority over the collection, use, and security of these important information systems on behalf of the public.

A number of uncertainties remain that may impact on privacy: (1) whether, and to what extent, public and private-sector third parties will seek to require REAL ID for proof of identity for purposes unrelated to the REAL ID Act and the final rule; (2) whether, and to what extent,

public and private-sector third parties will access and use, for purposes unrelated to the REAL ID Act or the final rule, the PII stored in the MRZ of a REAL ID credential; (3) how the State DMVs will conduct and govern the data verification of Federal databases required by the Act and the final rule (§37.13); and (4) how State DMVs will conduct and govern the State-to-State check necessary to determine if an applicant for a REAL ID cards holds a driver's license in another state (and if so has terminated or has taken steps to terminate that license) (§ 37.33(d)). This PIA discusses these privacy-related issues. The DHS Privacy Office may update this PIA as additional decisions are made on these issues.

Fair Information Practice Principles

The Privacy Act of 1974 imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Privacy Act also articulates concepts, known as the Fair Information Practice Principles (FIPPs), which are the generally recognized principles by which governments assess and mitigate privacy impacts on individuals. Section 222(2) of the Homeland Security Act of 2002, as amended, states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974. As such, the Privacy Office has developed a description of the FIPPs that underlies the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.

The DHS Privacy Office conducts PIAs on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002, as amended. This PIA is issued pursuant to Section 222(4), of the Homeland Security Act, which calls for the Chief Privacy Officer of the DHS to conduct a "privacy impact assessment of proposed rules of the Department." It examines the privacy impact of the REAL ID final rule as it relates to the construct of the FIPPs and offers a number of recommendations for DHS and the States to enhance privacy protections in light of the FIPPs. This PIA updates the PIA issued on March 1, 2007, in conjunction with the REAL ID NPRM.

1. Principle of Transparency

Transparency is the first and perhaps most important of the FIPPs. This principle calls for Federal agencies collecting personally identifiable information from individuals to be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance. Most importantly, there should be no system the existence of which is a secret. Transparency is followed in the final rule and PIA by providing the public with a description of the information practices associated with the implementation of the REAL ID Act. As noted in the final rule, DHS received over 21,000 comments on the NPRM. The final rule addresses the comments received during the 60-day public comment period. This PIA does not duplicate the comment summaries or responses but rather highlights how the final rule address the privacy issues outlined in the NPRM PIA. In addition, the "Privacy Considerations" section of the final rule (IV.D.) provides a general response to each of the areas noted in the NPRM PIA.

Although the final rule fully describes the nature and type of PII collected and used pursuant to the Act, final decisions have not been made regarding the operation and governance

of the architecture necessary to conduct the various data checks mandated under the verification requirements of the Act and the final rule. The final rule addresses ongoing discussions between DHS, Department of Transportation (DOT), the States and the American Association of Motor Vehicle Administrators (AAMVA) to establish a centralized verification system (a "hub") to assist States in conducting the required data verification checks against Federal databases and the State-to-State checks to ensure that a driver holds one and only one REAL ID credential. (See Sections II.C., IV.E., and IV.L. of the final rule.) Section II.C. indicates that DHS, in consultation with AAMVA, DOT, the Social Security Administration, the Department of State (DOS), National Association of Public Health Statistics and Information Systems (NAPHSIS), and State representatives, is working to define requirements for a network and messaging system or "hub" to support the data verification and State-to-State data check requirements of REAL ID.

The final rule identifies AAMVAnet, the network system AAMVA operates to facilitate data verification for the State DMVs, as a potential hub. The Privacy Office recognizes the importance of providing greater transparency regarding the architecture of this hub and how it will be governed. DHS and the States have not yet defined who will govern the hub and its business rules, such as: (1) who will have access to the hub; (2) how the hub and the information it handles will be used; (3) how individuals may access information about themselves held within the hub; (4) what security measures will be built into the system to ensure the data is protected; and (5) how the hub will ensure accountability to DHS and the public that all of the business rules are implemented and enforced. This PIA will be updated when information regarding these decisions becomes available.

Building upon AAMVA and the AAMVAnet system may offer the best opportunity to ensure that the States exercise maximum control over the operation and governance of the data checks mandated by the Act and the final rule. As described in the NPRM PIA, AAMVA, founded in 1933, 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.

DOT delegated operation of its Commercial Driver's License Information System (CDLIS) to AAMVA in December 1988, and it began operation in January 1989. DOT is currently funding an ongoing project to upgrade the capacity of AAMVAnet. Of particular importance from a privacy and security perspective is AAMVA's plan, as part of this upgrade, to build in security features such as end-to-end data encryption and full compliance with the Federal Information Security Management Act-based security standards. The DOT-funded project will provide the capability for AAMVAnet to potentially be expanded to provide the capacity to handle the increased transaction volume for the required State-to-State transactions. Most importantly, the AAMVAnet backbone resides on a private network with no connectivity to the Internet, making it a highly secure transportation layer for all communications between States and Federal agency databases. In addition, CDLIS already supports queries to every State DMV every time an individual applies for a driver's license, not just a commercial driver's

license, in any State or the District of Columbia. Moreover, as described in the preamble to the final rule, AAMVAnet already supports verification of both social security numbers (SSNs) and birth certificates for State DMVs. These application systems already enable States to query the Social Security Administration's (SSA) Social Security On-Line Verification (SSOLV) database and the Electronic Verification of Vital Events (EVVE) system owned and operated by the National Association for Public Health Statistics and Information Systems (NAPHSIS). While 47 States now verify SSNs through AAMVAnet, verification of birth certificates through NAPHSIS is currently limited to those few States whose vital events records are available online. In both cases, only State DMVs can initiate queries, personal information is verified and not exchanged, and no personal information is created, modified, or stored as a result of the transaction.

The United States Citizenship and Immigration Services Agency (USCIS) is now working to modify its Systematic Alien Verification for Entitlements (SAVE) system to meet the requirements of REAL ID. SAVE is an intergovernmental information-sharing initiative designed to aid eligibility workers in determining a non-U.S. citizen applicant's immigration status, and thereby ensure that only entitled non-U.S. citizen applicants receive Federal, State, or local public benefits and licenses. The SAVE Program is an information service for benefit issuing agencies, institutions, licensing bureaus, and other entities. The SAVE Program does not make determinations on any non-citizen applicant's eligibility for a specific benefit or license. Currently a majority of States have signed Memoranda of Understanding to access and use SAVE; however, each MOU is individually negotiated and tailored to the specific requirements of each State. USCIS is working to develop a standard user interface to meet all State DMV business process needs and to draft requirements for a common messaging system that takes advantage of the same AAMVAnet standards and infrastructure that support State DMV queries against SSOLV, EVVE, and other Federal and State databases. An updated PIA will be conducted on any changes made to SAVE related to REAL ID. (The PIA that addresses SAVE is posted at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_vis_update.pdf)

A primary privacy concern has been whether the REAL ID will result in a national identity system, including a centralized database of PII regarding all drivers. Although DHS cannot control how private sector third parties will use REAL ID cards, it can address the concern regarding the development of a centralized database. DHS states the following in the preamble to the final rule: "DHS does not intend that a REAL ID document become a *de facto* national ID based on the actions of others outside of DHS to limit their acceptance of an identity document to a REAL ID-compliant driver's license or identification card." Neither the REAL ID Act nor the requirements of the final rule expressly create a centralized database of all drivers' information. The REAL ID Act, however, requires that a State must refuse to issue a REAL ID-compliant card to an applicant who holds a driver's license from another State (without verifying that the other license has been terminated or the applicant has taken steps to terminate it). It would be easier for a State to meet this verification requirement through an index or pointer system, rather than checking with each State DMV individually. As discussed in the Privacy Considerations section of the preamble (Section IV.D.1.), it is currently technically and economically difficult to design a system that would avoid using an index or pointer system to direct the checks to the appropriate State. State systems would not be able to handle the volume of electronic messages received if all jurisdictions were sending and receiving messages

from all jurisdictions at the same time without such an index or pointer system. DHS will work to ensure that this central repository is only used to facilitate the State-to-State data checks or to permit access by authorized law enforcement personnel who are checking a specific license or identification card against the system and for no other purpose. The access rules to the still-to-be-built hub, for example, will help implement these protections. In addition, DHS will work to ensure that this index or pointer system will include the minimal amount of PII needed to facilitate effective querying and reduce the occurrence of false positives and false negatives.

The preamble provides a number of statements indicating that the States will play an important role in determining the governance structure of any system that may interface with the State licensing systems and the Federal verification systems, and that "DHS is mindful that the States expect to continue to have control over their systems, their information, and the processes that govern any use or access." (See preamble Section IV.E.) The Privacy Office supports these statements and believes that it is important for privacy that the States have a critical role in governing the architecture of these data checks with representation from the Federal agencies that operate the various verification databases. AAMVAnet is governed by the Board of AAMVA and is subject to the security and privacy requirements established by the association of DMVs. The Privacy Office has had the opportunity to meet with AAMVA and a number of its member States and believes the organization can appropriately address privacy concerns raised by the use of a hub to conduct the data checks REAL ID implementation requires, should a decision be made to contract with AAMVA for this purpose.

To improve transparency, the Privacy Office encourages DHS and AAMVA to provide the public with information on the implementation of the REAL ID architecture as it is developed. In addition, as recommended in the *Best Practices for Protection of PII* document, States should provide applicants for REAL ID cards with specific notice about what information is collected, how it will be used, and applicants' access and redress rights.

The Privacy Office supports having the States govern the operation of the data checks and using AAMVA as the hub for the reasons described above. The Privacy Office also recommends that DHS make public the final agreements and business requirements associated with the operations and governance of these data checks to provide transparency and earn the public's trust that privacy is addressed. Any sensitive information, the disclosure of which could undermine the security of the operation, could be redacted before making the agreements and business requirements public.

In addition to implementation of REAL ID, DHS is encouraging States to enter into voluntary agreements to produce enhanced driver's licenses (EDLs) that would serve as alternative documents to passports under the Western Hemisphere Travel Initiative (WHTI). These State-issued EDLs, intended to also meet REAL ID requirements, would be available only to U.S. citizens who voluntarily apply. DHS will be issuing a PIA specific to EDL projects and documents that utilize Radio Frequency Identification to facilitate cross border movement.

2. Principle of Individual Participation

This principle calls upon agencies that collect PII to involve the individual in the process of using his or her PII. In particular, to the extent practical, agencies should seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding its use. The proposed *Best Practices for Protection of PII* provides guidance to State DMVs on how to implement this principle.

It is often difficult to apply the individual participation principle where the government mandates collection of PII in order to obtain a benefit. In such instances, the government may need the PII in order to ensure that the right individual receives the right benefit, in this case a driver's license or State-issued ID. Although REAL ID is a voluntary program for the States, it is not necessarily voluntary for individuals who want to obtain a driver's license so that they can legally drive unless their State also provides an alternative non-compliant credential, which some States may issue for a number of different reasons, such as licensing residents who cannot document lawful status. It is likely that the types of PII DMVs will collect will be very similar for REAL ID and non-REAL ID compliant cards and that both types of cards will have a MRZ containing PII that is not encrypted or protected from third party skimming. Despite these similarities, some individuals may still choose to have a non-REAL ID driver's license.

At the Federal level, pursuant to the Privacy Act of 1974, individuals may request access to information held by the various Federal programs participating in the REAL ID implementation, including the SAVE and SSOLV systems. At the State level, States generally have access laws that enable individuals to request access to their DMV information and an opportunity to correct their records if there is an error. State DMVs direct applicants to the appropriate Federal agency -- SSA to verify SSNs or USCIS to verify immigration status -- to handle errors in Federal records. As described in the final rule, SSA and USCIS have redress programs in place to assist individuals whose records are incomplete or inaccurate. For example, an individual who believes that information about them in SAVE is inaccurate, can schedule an appointment online with USCIS at www.uscis.gov and be assigned an appointment at their designated immigration office based on the individual's residential zip code. These appointments afford an individual an opportunity to meet with an Immigration Officer face-to-face to resolve any non-asylum related issues relating to their current or pending immigration case. Minimal information, including an Alien Registration Number or Receipt Number is required to schedule an appointment. In addition, DMVs conduct State-to-State record checks when processing a new applicant; however, when an applicant needs to seek access to his or her out-of-State DMV record, the applicant must make the request directly to the State DMV. DHS states in the final rule that it will work with the States to inform the public of the States' ability to access and correct DMV records as well as records held in the various Federal data verification systems used to implement the REAL ID.

3. Principle of Purpose Specification

This principle requires agencies to specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used. The final rule states that its purpose is to establish minimum standards for State-issued driver's licenses and identification cards that Federal agencies will accept for "official purposes" after May 11, 2008, in accordance with the REAL ID Act of 2005. The Act authorizes the Secretary of DHS to define "official purposes"; and in the final rule, DHS adopts only the three purposes expressly stated in the Act -- accessing Federal facilities, boarding Federally-regulated commercial aircraft, and entering nuclear power plants.

Many of the comments filed raised the concern that the REAL ID implementation will result in a national ID. As noted above in the Transparency Section, the preamble expressly states that DHS does not intend that a REAL ID document become a *de facto* national ID or support the creation of a national ID card. (See preamble discussion of "Definition of 'Official Purpose.'" (IV.B.1.))

4. Principle of Minimization

Application of this principle in the context of the REAL ID requires that the States only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). The REAL ID Act specified the PII to be collected and displayed on the credential, a retention schedule for the documentation applicants provide, and the document verification required to obtain the REAL ID credential. In light of comments received, however, the final rule has made several substantive changes from the NPRM to reduce the amount of PII collected and stored, minimizing the data collected to that required by the Act.

First, the final rule has dropped the requirement to conduct financial background checks for covered DMV employees. The NPRM had included financial checks as part of its implementation of the Section 202(d)(8) requirement for DMV employees authorized to manufacture or produce drivers' licenses and identification cards to undergo "appropriate security clearance requirements." Section 37.45 of the final rule now requires all covered employees to undergo a name-based and fingerprint-based criminal history records check and an employment eligibility check, as well as a prior employment reference check if the individual has been employed by the DMV for less than two consecutive years. Section 37.45 of the NPRM proposed that States conduct a lawful status check using SAVE. The final rule, however, requires an employment eligibility check and recommends, but does not require, that the States participate in the E-Verify program or any successor program for employment verification eligibility. The preamble explains that this change reflects the fact that employment eligibility verification using the standard Form I-9 is required for all employees (whether U.S. citizens or aliens) hired to work at DMVs (or any other U.S. employer) and that lawful status is defined for REAL ID purposes in a way that is not synonymous with employment eligibility under the Immigration and Nationality Act. The rule, therefore, now cross-references the current Form I-9 requirements rather than requiring a new check through SAVE.

Second, several provisions in the final rule help to limit the amount of information States will need to collect in order to implement the regulations. As noted above, the REAL ID Act directs what information States must collect and what information is contained on the cards. Section 202(b) of the Act directs that REAL-ID compliant licenses and identification cards include the following information: the applicant's full legal name, date of birth, and gender; driver's license or identification card number; a digital photograph of the applicant; the applicant's address of principle residence; the applicant's signature; physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes; and a common machine-readable technology, with defined minimum elements.

The Act defines the minimum elements to include on the cards in § 202(b), but does not define the elements to include in the MRZ, directing DHS to define those elements in its rulemaking. A number of commenters recommended limiting the data elements in the MRZ, and one suggested only including a pointer in the MRZ to link to a database limited to law enforcement. From a privacy perspective, implementing a pointer system may seem preferable; however, implementing such a system would require a centralized national database since law enforcement from all jurisdictions would need access to the data, and all law enforcement would need the technology to enable access to the database from their patrol cars or motorcycles, which is currently not possible from more rural or mountainous areas of the country. To meet the needs of the DMVs and law enforcement, § 37.19 of the final rule specifies that the MRZ contain the following data elements: expiration date; holder's full legal name, except as permitted under § 37.11(a)(2); transaction date; date of birth; gender; address as listed on the card pursuant to § 37.17(f); unique driver's license or identification card number; card design revision date; inventory control number of the physical document; and State or territory of issuance. Several provisions of the final rule provide data limitations pertaining to the MRZ. For example, in response to comments, the final rule has eliminated the proposed NPRM requirement to include name history in the MRZ. In addition, § 37.17(d) now makes clear that the unique license or card identification number must only be unique to each license or card holder within the State and not unique across all the States and other covered jurisdictions. This provides further evidence that REAL ID does not seek to become a national ID.

Third, the final rule provides States with broad authority to protect the confidentiality of the address of principal residence for certain classes of individuals consistent with applicable State law. To make this clearer, DHS has added language to the final rule enabling State DMVs to apply an alternative address on a license or ID if the individual's address is entitled to suppression under State or Federal law or suppressed by a court order including an administrative order issued by a State or Federal court. The individual's true address must be captured and stored in a secure manner in the DMV database when an alternative address appears on the face and MRZ of the ID. (See § 37.17(f) of the final rule and Section IV.I.4. of the preamble.)

Fourth, the minimization principle also requires that the data should only be retained for as long as necessary and relevant to fulfill the specified purposes. Section 202(d) of the Act requires States to (1) employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format and (2) retain paper copies of source documents for a minimum of seven years or images of source documents

presented for a minimum of ten years. Section 37.31(a) of the final rule carries forward these requirements and provides States with the option of paper (minimum of seven years), microfiche (minimum of ten years), or digital images (minimum of ten years). In addition, § 37.11(a)(1) of the final rule reduces the retention period for the photograph and identity of individuals denied a license from ten years, as proposed in the NPRM, to five years. The final rule states that this limited retention is necessary to enable State DMVs to reduce the incidence of individuals who shop among DMVs until one of them issues a license.

Finally, in a new rule provision, States, at the request of an applicant or on a State's own initiative, may retain a copy of the birth certificate that redacts confidential information not related to establishing the identity and birth date of the applicant. (§ 37.31(c). This provision will help protect medical and other personal information not relevant to REAL ID.

5. Principle of Use Limitation

This principle requires the States and DHS to use PII solely for the purpose(s) specified in the Act and the rule and for which the individual has received notice. The *Best Practices for Protection of PII* guidance outlines the content of a meaningful notice to the individual. (See Attachment A.) Section 37.41(b)(2)(ii) of the final rule specifically requires States as part of the security plan to provide a "privacy policy regarding the personally identifiable information collected and maintained by the DMV pursuant to the REAL ID Act." This policy will serve to inform the public of the States uses of the PII collected by the States and, as recommended in the *Best Practices for Protection of PII guidance*, should be captured in a written notice given to each applicant for a REAL ID card.

In addition, the PII collected to implement this rulemaking should only be used for the purposes of law enforcement, verification of personal identity, or highway and motor vehicle safety. Section 37.41 (b)(2)(i) of the final rule calls for the States to protect the DMV records and information systems and provide safeguards to prevent unauthorized access, use, or dissemination of applicant information and images of source documents.

Of particular privacy concern, however, is how the PII contained in the State-to-State data verification index or pointer system will be used by DHS, the States, or other entities, if , given access to it. Setting limitations on the use of the PII in the index should be the first item of business for the governance body established to operate and oversee the State-to-State data verification system. The Privacy Office intends to monitor the work of the governance body and to provide privacy guidance as appropriate. The central index or pointer system should not be used, for example, by any Federal or State agency for intelligence, data mining, or "fishing expeditions." Rather, access should be limited to targeted law enforcement or DMV investigations or verification of an individual's identity based on a "need to know," as outlined in the Privacy Act and many similar State privacy acts.[2]

[2] Some Federal law enforcement officers, principally Federal Motor Carrier Safety Assistance Program (MCSAP) officers, have access to CDLIS now via DOT's Federal Motor Carrier Safety Administration's access to CDLIS. The majority of other law enforcement officers, however, do not access CDLIS but rather access driver history records via Nlets. Nlets, a 501(c)(3) not-for-profit organization owned and governed by the States, is a computer-based message switching system that links together State, local and Federal law enforcement and justice agencies for

NPRM § 37.33(b), which authorized electronic access by States to each others' databases has been withdrawn from the final rule. While the language of this section was directly pulled from § 202(d)(12) of the Act, privacy groups and some of the States filed comments expressing concern with the section's possibly broad scope. In response, the preamble to the final rule states that the REAL ID Act does not authorize a State to access personal information contained in the DMV database of another State, but rather permits States to use existing processes to request transfer of a prior motor vehicle record when an applicant is moving his or her license from one State to another.

Finally, § 37.41(b)(2)(iii) of the final rule sets the Driver's Privacy Protection Act (DPPA)(18 U.S.C. § 2721 *et seq*.) as a protective floor to limit the use of the information in the DMV databases, but then expressly recognizes that States can do more: "State plans may go beyond these minimum privacy requirements to provide greater protections, and such protections are not subject to review by DHS for purposes of determining compliance with this Part." The DPPA prohibits DMVs from disclosing "personal information" contained in a DMV "motor vehicle record," unless the disclosure falls within fourteen permissible uses, including disclosure to any Federal, State, or local government agency to carry out that agency's legitimate functions. Given the fourteen wide-ranging permissible uses, the DPPA really only serves as a limitation on the sale of the personal information found in motor vehicle records for marketing purposes. (DMVs must obtain express consent for sale of record information for marketing purposes.) Therefore, the Privacy Office recommends that the States not rely solely on the DPPA to fully protect the privacy of the personal information required under the REAL ID Act. The Privacy Office urges the States to examine their implementation of the DPPA and, to the extent possible, further limit and monitor the disclosure of the PII in order to enforce these resale and redisclosure prohibitions. The FIPPs principle of use limitation calls for limiting disclosure to those purposes "compatible" with the purpose for which the PII was collected. The final rule expressly recognizes the States authority to provide greater protections than set by the DPPA, and the Privacy Office urges the States to do so.

6. Principle of Data Quality and Integrity

This principle calls on DHS and the States to ensure, to the extent practical, that PII is accurate, relevant, timely, and complete, within the context of each use. In large part, data quality and integrity underscore the very purpose of the REAL ID regulations – to reduce fraudulent cards. The complex system of data verification required by REAL ID will likely improve the accuracy and validity of the cards. State DMVs will still face the challenge of detecting falsified source documents; however, through data verification, it is likely that the number of fraudulently issued cards will be reduced significantly. The redress process discussed above in the Individual Participation Principle section of the PIA, however, will be very important to address "no match" problems, which will invariably occur given the volume of data checks and the data quality limitations of the various Federal (USCIS, DOS, SSA) and not-for-profit (NAPHSIS' Electronic Verification of Vital Events) databases involved. DHS will work

---

the purpose of information exchange. Nlets allows law enforcement to seek a driver's record (driver history information and vehicle registration information) from a State of record's Department of Safety, which then routes the queries to a DMV via an internal State network.

closely with the States to inform the public of the availability of redress to address data quality limitations. Finally, the tamper-resistant features the States will adopt for the REAL ID cards should enhance their integrity and increase government and public confidence in the cards.

7. Principle of Security

To satisfy this principle, DHS and the States must ensure that PII (in electronic or hard copy form) is protected through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. The final rule addresses this principle with regard to the security of State DMV databases associated with REAL ID. As noted above, the decisions on the "hub" have not yet been finalized; once completed, a future PIA will address the security safeguards provided to protect PII.

Protection of the PII held in State DMV databases and in the data verification systems

Section 37.33(b) of the final rule expressly requires that States protect the information collected pursuant to the REAL ID Act, and § 37.41 requires States to prepare, for purposes of REAL ID certification, a security plan for all State DMV facilities and systems involved in the enrollment, production, or issuance of the REAL ID card. Section 37.41(b)(2) sets forth the minimum contents for the protection of PII, including, but not limited to:

(1) Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act;

(2) Safeguards to include procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction;

(3) A privacy policy regarding the PII collected and maintained by the DMV pursuant to the REAL ID Act;

(4) A prohibition on release and use of personal information that, at a minimum, is consistent with the Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.*;

(5) Access controls, including the following:

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

(b) Employee background checks.

(c) Controlled access systems.

(6) Periodic training in fraudulent document recognition for all covered employees engaged in the issuance of driver's licenses and identification cards and security awareness training, including threat identification and handling of Sensitive Security Information (SSI);

(7) Emergency/incident response plan;

(8) Internal audit controls; and

(9) An affirmation that the State has both the authority and the means to protect the confidentiality of REAL ID driver's licenses or identification cards issued for select persons requiring confidentiality in support of their official duties.

Although not specified in the final rule, the Privacy Office encourages States to include breach notification as part of the required "emergency/incident response" plan. Many State laws already require such notification, and breach notification is consistent with recent Office of Management and Budget policies governing Federal agencies.

The final rule classifies the security plan required by § 37.41 as containing Sensitive Security Information (SSI) and requires States to handle and protect the plan in accordance with the SSI requirements in 49 CFR Part 1520. To the extent the security of the information is not undermined, States are encouraged to inform the public through their privacy policy about the protections provided for the personally identifiable information. The Privacy Office supports the enumerated protections in the security plan and believes that they provide a solid plan for protecting the PII collected and stored at the State DMVs.

Moreover, the Privacy Office recommends that States consider adopting protections similar to those applied to SSI for the information held in the hub and formalize those protections through a Memorandum of Agreement with the operator of the hub to ensure the PII contained in the hub is fully protected. If, as the Privacy Office recommends, the operation and governance of the hub lies with the States, the requirements of the final rule in combination with these Federal requirements will provide the necessary layers of protection for this sensitive collection of PII.

Protection of the PII in the MRZ

As discussed in the preamble for the final rule, the REAL ID Act does not authorize DHS to prohibit third-party private-sector uses of the information stored on the front of the REAL ID card or on the MRZ. (IV.I.7) The preamble states that DHS recognizes that a 2D barcode, the technology selected for the MRZ, may have security vulnerabilities and technology limitations compared to other available technologies; however, it selected the PDF 417 2D barcode because it is already used by 45 jurisdictions and law enforcement officials across the country, and a different technology choice would hamper law enforcement efforts and may pose an additional financial burden on the States. To address the privacy concern, the preamble discusses the role States can play in limiting the use of the MRZ. For example, California, Nebraska, New Hampshire, and Texas currently limit third party use of the MRZ, and AAMVA has issued a model Act limiting such use. The preamble encourages other States to take similar steps to protect the information stored in the MRZ from unauthorized access and collection.

The preamble also discusses the issue of employing encryption to protect the PII contained in the MRZ. In the NPRM PIA, the Privacy Office urged DHS to adopt encryption to protect the PII on the MRZ from skimming by third parties other than law enforcement or DMVs. In the preamble to the final rule, DHS discusses the many comments filed for and against encryption and acknowledges that the skimming of the PII from the MRZ raises important privacy concerns. Nevertheless, DHS determined that given law enforcement's need for easy access to the information, and the complexities and costs of implementing an encryption

infrastructure, it would not require encryption of the MRZ at this time. DHS does announce in the preamble, however, that if the States collectively determine that it is feasible to introduce encryption in the future, DHS will consider such an effort, so long as the encryption program enables law enforcement easy access to the information in the MRZ. Moreover, the preamble states that DHS in consultation with the States, DOT, and after providing for public comment, is open to considering technology alternatives to the PDF 417 2D bar code in the future to provide greater privacy protections. The Privacy Office supports efforts to find a practical and effective technological means of protecting the PII on the MRZ as well as State actions to limit the skimming of this PII.

8. Principle of Accountability and Auditing

The final principle calls on DHS and the States to be accountable for complying with all of the FIPPs, providing training to all employees and contractors who use PII, and to audit the actual use of PII so as to demonstrate compliance with these principles and all applicable privacy protection requirements. This principle requires programs to institute mechanisms such as training and audits to ensure that privacy protections are implemented. Section 37.51 of the final rule specifies a number of requirements for State certification. It includes two compliance checklists. The first is the Material Compliance Checklist, which is Appendix A to the final rule and is open to public comment. It will document State progress toward meeting DHS compliance benchmarks, including the security plan, and will serve as the basis for DHS approval of additional implementation extensions to May 11, 2011. The second is the Final Certification Checklist, which is mentioned in § 37.55(a)(1) of the final rule and will give States a simple form to document compliance with all of the requirements of Subparts A through D of the rule, including the security plan. DHS will use the certification process as the key means to ensure adherence to the rule. In addition to the checklists, State DMVs must regularly conduct audits of their programs and policies, which will provide a second layer of accountability. With regards to training, § 37.41(b)(5)(i)-(ii) requires all employees handling source documents or issuing REAL ID cards to attend and complete AAMVA approved (or equivalent) fraudulent document recognition training and security awareness training. Finally, but as yet undefined, will be the role of the body established to govern and operate the hub. This body can provide much needed oversight to ensure the hub protects the PII used in the State-to-State data checks and the messaging system for the data verification of Federal databases, as well as the privacy of the individuals to whom the information pertains. The Privacy Office will update this PIA when those decisions are finalized.

Rulemaking Contact

Darrell Williams, Director REAL ID Program Office
DHS Policy Office

Approval Signature Page

Original signed and on file the DHS Privacy Office
John Kropf
Acting Chief Privacy Officer
Department of Homeland Security

Attachment A

Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the Real ID Act

Privacy Best Practices

a. *Purpose*.

(1) *Purpose*. The Department of Homeland Security (DHS) Privacy Office issues these best practices as a guide to assist the States in protecting the privacy of the personally identifiable information associated with the implementation of the REAL ID Act. These practices incorporate standards and practices equivalent to those required under the Privacy Act of 1974 (5 U.S.C. § 552a) and other Federal and State laws that implement the Fair Information Principles. These practices are intended to supplement the limited protections of the Driver's Privacy Protection Act, 18 U.S.C. §2721 *et. seq*.

b. *Guidelines for Protecting Privacy*. Each State should develop, implement, and maintain policies and practices that adhere to the following Fair Information Practice Principles:

(1) *Transparency Principle*. This principle requires each State not to collect personally identifiable information in secret and to clearly and conspicuously disclose a State's policies and practices with respect to its handling of all aspects of the personally identifiable information held by a State DMV. To this end, each State should provide a written Privacy Policy Statement to each applicant at the time of application for a new, duplicate, modified, or renewed REAL ID driver's license or identification card. The Privacy Policy Statement should also be available to the public on the DMV website, adjacent to the online application, with a clear and prominent link. The Privacy Policy Statement should be clear, understandable, and include at least the following elements:

i. The types of personally identifiable information required to obtain a REAL ID driver's license or identification card, including data elements required by State laws and regulations and by the regulations implementing the REAL ID Act of 2005, and with respect to each element, whether providing it is mandatory or voluntary;

ii. Identification of the Federal information systems against which the personally identifiable information provided on the application and in documentation presented to obtain a REAL ID driver's license or identification card will be checked for accuracy;

iii. The existence of the machine-readable zone on the license or identification card and the types of personally identifiable information contained therein and that such information is not secured and can be read by any third party that runs the credential through a card reader, unless the information is encrypted;

iv. The authority, statutory or other, for the collection of each type of personally identifiable information;

v. The retention period for maintaining the personally identifiable information;
vi. The specific purposes for which the personally identifiable information is collected, including the purpose of driver licensing and the Federal purposes enumerated in the REAL ID Act of 2005;
vii. The foreseeable disclosures of the personally identifiable information to other State DMVs and to law enforcement;
viii. The procedures by which a State will notify individuals of material changes to the information practices to the Privacy Policy Statement, including the ability to consent or opt-out, as appropriate;
ix. The right of individuals to review their own personally identifiable information and to request correction of inaccurate, incomplete, or irrelevant information; and
x. The procedure for individuals to request redress, including contact information of an official responsible for redress. The opportunity to seek redress should be widely available, easy-to-use, and staffed to provide prompt and accurate response.

(2) *Individual Participation Principle*. This principle requires that an individual have the right to (a) obtain confirmation of whether or not a State has personally identifiable information relating to him; (b) have access to the personally identifiable information related to him within a reasonable time, cost, and manner and in a form that is readily intelligible to him; (c) be given an explanation if a request made under (a) and (b) is denied and be able to challenge such denial; and (d) challenge personally identifiable information relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

i. Each State should demonstrate that it has adopted effective and timely procedures to permit each holder of, or applicant for, a REAL ID driver's license or identification card the opportunity to examine the personally identifiable information that is on file concerning such license or identification card holder, and to obtain a copy of such information, upon request.
ii. Each State should demonstrate that it has adopted effective and timely procedures to permit each holder of, or applicant for, a REAL ID driver's license or identification card to request the making of corrections to personally identifiable information that is on file, and to receive a substantive response to such a request.
iii. Each State should demonstrate that it has a redress process in place to address requests to make corrections to State DMV records and to assist individuals whose applications for a REAL ID driver's license or identification card are denied due to implementation of this Rule.
iv. These guidelines should not be construed to require any State to disclose information from the record of a REAL ID driver's license or identification card, or to make corrections to any such record, where

such action or actions would conflict with the objectives of any official law enforcement investigation or administrative or judicial proceeding.

(3) *Purpose Specification Principle*. This principle requires that the State specify at the time of collection the purpose(s) for collecting personally identifiable information. The notice of such purposes is provided in the Privacy Policy Statement. Its subsequent use should be limited to the fulfillment of those purposes or such others that are compatible with those purposes stated in the Privacy Policy Statement unless individuals are given written notice of the proposed change in use and individuals provide express written consent to its use for such new purpose.

i. Unless otherwise authorized by law, each State should limit its use of personally identifiable information related to the implementation of the REAL ID Act regulations to the performance of official responsibilities pertaining to law enforcement, the verification of personal identity, or highway and motor vehicle safety.
    a. Unless otherwise authorized by law, a State should request and transmit personally identifiable information related to the implementation of the REAL ID Act to another State only for the purpose of identity verification, and for other related, official DMV purposes.

ii. Each State should inform each individual applicant, including each applicant for renewal of a driver's license or identification card, that personally identifiable information in the record of such applicant may be transmitted to other DMV and law enforcement agencies only if such disclosure is related to the performance of official responsibilities pertaining to law enforcement, the verification of personal identity, highway and motor vehicle safety, or any other official purpose expressly authorized by law.

iii. The personally identifiable information contained in the machine-readable zone of the license or identification card document should be limited to the data elements visible on the face of the credential, unless the State is authorized or required by State or Federal law to place additional personally identifiable information in such machine-readable zone.

iv. As noted above, the Privacy Policy Statement should inform each individual applicant, including each applicant for renewal, of the existence of the machine-readable zone on a REAL ID license or identification card and of the types of personally identifiable information contained therein, and that it is not secure and can be read by any third party that runs the credential through a card reader, unless the information is encrypted;
    a. States should consider limiting by law the ability of third parties, other than official law enforcement officers, to scan and retain the personally identifiable information stored in the machine-readable zone without the express consent of the holder of the license or identification card.

(4) *Minimization Limitation Principle*. This principle requires that each State DMV only collect the personally identifiable information necessary for official DMV purposes as stated in the Privacy Policy Statement. In addition, each State DMV should only obtain such personally identifiable information by lawful and fair means and, to the greatest extent possible, with the knowledge or consent of the individual applicant/cardholder.

i. Each State should collect from each individual applicant/cardholder only the personally identifiable information specified in the implementing regulations for the REAL ID Act of 2005, unless the State is required or authorized by applicable law to collect one or more additional types of information.
    1. If a State is required or authorized by applicable law to collect one or more types of personally identifiable information not specified in the implementing regulations for the REAL ID Act of 2005, the State should have procedures in place to maintain the confidentiality of such additional information in accordance with these Privacy Guidelines and applicable State laws.
    2. Each State should inform each individual applicant /cardholder in writing, on the driver's license or identification card application form, that the Social Security Number (SSN) is obtained and used solely for the purpose of the verification of identity and will not be disclosed except as expressly authorized by law.
        a. Each State should inform each individual applicant/cardholder that the SSN will not appear on the driver's license or identification card (or in the MRZ).
        b. Each State should inform each individual applicant/cardholder that the SSN provided on the application and in documentation provided to request a license or identification card will be verified against the records of the U.S. Social Security Administration.
    3. With reference to the collection of digitized images, each State should inform each individual applicant/cardholder that his or her image will be checked against the images on file with the DMV, or any Federal verification system, in order to protect against identity theft, if such a check is conducted.
        a. Each State should also inform each individual applicant/cardholder that his or her image may be exchanged with other State DMVs or law enforcement authorities in other jurisdictions but only for the purpose of identity verification and in order to deter fraud and identity theft, if such a check is conducted.

(5) *Use Limitation Principle*. This principle requires that each State only use the personally identifiable information for the purposes and uses originally specified in the Privacy Policy Statement, except (a) with the express consent of the

individual applicant or credential holder, or (b) as authorized by law. This includes limiting disclosure of the information to the purposes and uses specified in the Privacy Policy Statement.

i. As noted in the *Purpose Limitation Principle* above, unless authorized by law, no State should disclose personally identifiable information related to the implementation of the REAL ID Act except to a governmental agency engaged in the performance of official responsibilities pertaining to law enforcement, the verification of personal identity, or highway and motor vehicle safety. (Disclosure to third parties is governed by the Driver's Privacy Protection Act 18 U.S.C. §2721 *et. seq*., however, States can provide additional protections.)

ii. No State should disclose personally identifiable information to a governmental agency or any authorized third party, unless the requestor has identified the office(s) and the individual(s) that are authorized to obtain such personally identifiable information.

a. No State should disclose personally identifiable. information to a governmental agency or any authorized third party, unless the requestor has provided sufficient information to accurately identify the record that is being sought, in accordance with the State's written protocols for exchange of records.

b. No State should disclose personally identifiable information to a governmental agency or any authorized third party that has not entered into a written agreement with the State unless required by law.

c. Each State should demonstrate that it has implemented a procedure to notify all affected individuals promptly of incidents of the unauthorized disclosure, theft, or loss of personally identifiable information held by a State DMV, and to provide appropriate relief to such individuals.

d. Each State should adhere to the terms and conditions of the agreements for access to the various Federal information systems used to verify the data presented to obtain a REAL ID credential.

(6) *Data Quality and Integrity Principle*. This principle requires that the personally identifiable information collected, used, and maintained related to implementation of this Rule be relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, it be accurate, relevant, complete, and up to date.

i. Each State should develop standards to ensure that the personally identifiable information used in making any determination about any individual applicant to obtain a REAL ID credential is as accurate,

relevant, timely, and complete as is reasonably necessary to assure fairness to the individual in such determination.

ii. Prior to disseminating any record containing personally identifiable information about an individual, each State should make reasonable efforts to assure that such record is accurate, complete, timely, and relevant for the purpose for which it is being disclosed.

(7) *Security Safeguards Principle*. This principle requires that personally identifiable information should be protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure. (See Security Best Practices below for security safeguards.)

(8) *Accountability and Auditing Principle*. This principle requires that each State that collects and manages personally identifiable information be held accountable for compliance with the State's privacy, including security, policies related to implementation of the REAL ID Act of 2005 and its implementing regulations. In addition, each State should be responsible for identifying, training, and holding agency personnel accountable for adhering to agency information quality and privacy policies related to implementation of the Act.

i. Each State should be responsible for implementing these best practices consistent with each State's individual applicable State privacy laws and regulations.

ii. Each State should report to DHS in a timely manner any negative finding by an auditor that is material to compliance with the privacy requirements of the implementing regulations of the REAL ID Act of 2005 as part of its annual REAL ID Certification.

iii. Each State should obligate its suppliers and other contractors that handle personally identifiable information related to the implementing regulations of the REAL ID Act of 2005 to comply with the same privacy and security guidelines that apply to the State.

(c) *Privacy Impact Assessment*. Each State should conduct a Privacy Impact Assessment (PIA) to identify and analyze how personally identifiable information related to the implementing regulations of the REAL ID Act of 2005 is collected, used, maintained and protected to ensure that these best practices are fully implemented. At a minimum, the PIA should address:

(1) What information is to be collected;
(2) Why the information is being collected;
(3) The intended use of the DMV of the information;
(4) With whom the information will be shared;
(5) What notice or opportunities for consent will be provided to individuals regarding what information is collected and how that information is shared;
(6) How the information will be secured.

Information Security Best Practices

(a) *Purpose.*

(1) *Purpose*. DHS issues these best practices as a guide to assist the States in developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information related to the State DMV's implementation of the Real ID Act of 2005. These practices incorporate standards and practices intended to be [consistent with/equivalent to] those required for Federal information systems under the Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3542) and the information security standards issued by the National Institute of Standards and Technology (NIST), including the Federal Information Processing Standards Publication (FIPS PUB 200) and the NIST Recommended Security Controls for Federal Information Systems (NIST 800-53).

(b) *Guidelines for Safeguarding Personally Identifiable Information.*

(1) *Information security program*. Each State should develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to the implementation of the REAL ID Act's regulations. Such safeguards should include the elements provided in the following section and should be reasonably designed to achieve the following objectives:

i. Insure the security and confidentiality of personally identifiable information collected, used, or maintained related to the implementation of the REAL ID Act's implementing regulations;
ii. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
iii. Protect against unauthorized access to or use of such information.

(c) *Elements.*

(1) In order to develop, implement, and maintain a comprehensive information security program for purposes of implementation of the REAL ID Act's regulations, each State should include in its information security program the following elements:

i. Conduct periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of personally identifiable information and information systems that support the operations and assets of the State DMV necessary for implementation of the REAL ID Act's regulations;
ii. Develop and implement policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each such information system;
iii. Develop and implement plans to provide adequate information security for facilities, networks, information systems, or groups of information systems, as appropriate;
iv. Develop and implement an enterprise security program that addresses all of the following areas:

1. System access controls, which allow only authorized persons to access the personally identifiable information;
2. Computer and operations management, which implements practices to protect the personally identifiable information and ensures operational integrity;
3. System development and maintenance, which develops procedures for protecting information security and privacy in coding, testing, and maintaining information systems;
4. Physical and environmental security, which provides safeguards to protect the locations, buildings, and areas containing the technology equipment and information resources;
5. Compliance, which employs methods for monitoring and auditing compliance with this Rule, as well as responding to suspected instances of non-compliance;
6. Personnel security, which implements controls to assure that personnel are properly vetted for handling information systems;
7. Asset classification and control, which categorizes personally identifiable information systems as moderate or high sensitivity and implements security procedures, including data retention and destruction methods appropriate for the designated classification.

v. Conduct security and privacy awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the DMV) of the information security risks associated with their activities and their responsibilities in complying with DMV policies and procedures designed to reduce these risks;
vi. Conduct periodic testing and evaluation (audits) of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
vii. Develop and implement a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the DMV;
viii. Develop and implement procedures for detecting, reporting, and responding to security and privacy incidents, including a breach notification plan; and
ix. Develop and implement plans and procedures for continuity of operations for information systems that support the operations and assets of the DMV.

Background Resources for the Information Security Practices

Federal Information Processing Standards Publication - FIPS PUB 200 (March 2006) FIPS PUB 200 identifies the following minimum security requirements for federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:

(i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems.

Specifications for Minimum Security Requirements

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must: (i) establish and maintain baseline

configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.