Comments of the

DHS Data Privacy & Integrity Advisory Committee

Regarding the Notice of Propose Rulemaking

For Implementation of the REAL ID Act

The REAL ID Act is one of the largest identity management undertakings in history. It would bring more than 200 million people from a large, diverse, and mobile country within a uniformly defined identity system, jointly operated by state governments. This has never been done before in the USA, and it raises numerous policy, privacy, and data security issues that have had only brief scrutiny, particularly given the scope and scale of the undertaking.

It is critical that specific issues be carefully considered before developing and deploying a uniform identity management system in the 21st century. These include, but are not limited to, the implementation costs, the privacy consequences, the security of stored identity documents and personal information, redress and fairness, "mission creep", and, perhaps most importantly, provisions for national security protections.

The Department of Homeland Security's Notice of Proposed Rulemaking touched on some of these issues, though it did not explore them in the depth necessary for a system of such magnitude and such consequence. Given that these issues have not received adequate consideration, the Committee feels it is important that the following comments do not constitute an endorsement of REAL ID or the regulations as workable or appropriate.

The REAL ID Act of 2006 requires states to issue new driver's licenses by May 2008. The stated goals of this legislation are to assist law enforcement by providing nationwide uniformity in the driver's licenses and to reduce the risk of identity theft. To achieve this stated benefit, the law requires the Department of Homeland Security to issue regulations with three goals. First, the regulations must articulate the minimum requirements that each new driver's license must have. Second, the regulations will require states to validate the documents an individual uses to obtain a drivers license. Third, the regulation must establish a system so that each state can have access to the drivers' license database of another state.

Pursuant to the REAL ID Act, the Department of Homeland Security has promulgated a Notice of Proposed Rulemaking (NPRM) seeking public comment on the proposed rule and answers to a number of questions on a variety of issues. This Committee has reviewed the proposed rule and has several significant concerns about the proposed rules' Comprehensive Security Plan, the information stored in the Machine Readable Zone, one state's access to the driver's license databases in other states, and background checks for employees of facilities that will manufacture and produce the new driver's licenses. The issues pose serious risks to an individual's privacy and, without amelioration, could undermine the stated goals of the REAL ID Act.

I. Background

On April 4, 2007, the DHS Chief Privacy Officer tasked the Data Privacy and Integrity Advisory Committee to comment on the NPRM issued by DHS for implementation of the REAL ID Act. The Chief Privacy Officer asked that the Committee provide comments in several areas. They include the nature and

content of the policies and procedures that the Department should require States to provide in their Comprehensive Security Plans and on the types of information and the methods of storing that information in the Machine Readable Zone. They also include the best practices for developing a state-to-state system that addresses privacy protections, including security and access controls for data exchange. Finally, they include the guidance DHS should issue regarding the proposed requirement that the states conduct a background check.

The specific instructions to the committee read as follows:

> *Given the advisory role of the DPIAC and the significance of this rulemaking, we are asking that the DPIAC consider and provide recommendations to the Department on ways to enhance privacy when implementing the Act. Specifically, we are tasking the Committee to address the following issues:*
>
> *(1) Please provide comment regarding the nature and content of the policies and procedures that DHS should require states to provide in the Comprehensive Security Plan to protect the privacy of the personal information related to implementation of the REAL ID Act. (See NPRM Proposed Rule § 37.41 and MPRM Preamble section II.K.)*
>
> *(2) Please provide comment on what personal information should be stored and how it should be stored on the machine readable zone (MRZ) of the licenses and identification cards so that it can be protected from unauthorized collection and use. (See NRPM Preamble section II.H.7-9 and section II.B of the PIA)*
>
> *(3) Section 202(d)(12) of the Act requires states provide electronic access to all other states to information contained in the state's motor vehicle database. Please provide comment as to best practices for developing a state-to-state system where privacy protections, including security and access controls for data exchange are addressed.*
>
> *(4) Please provide comment on what guidance DHS should issue regarding the proposed requirement that the states conduct a financial history check. (See NPRM Proposed Rule § 37.45(b)(2) and NPRM Preamble section II.K.1.)*

I. Policies and Procedures in the Comprehensive Security Plan

Protecting personal information is a component responsibility for those who collect and store it. Security safeguards to prevent unauthorized access, use, disclosure or corruption of the information are a fundamental principle of not only of information security, but also of information privacy. The proposed rule requires that each state seeking to issue REAL ID's must submit a Comprehensive Security Plan. The Comprehensive Security Plan has two intentions. First, it requires security safeguards to prevent confidential information from unauthorized access, use, sharing, or compromise. Second, it requires personal information to be managed in specific ways designed to promote the privacy of the individuals involved.

A. Security Safeguards

With respect to security standards, the proposed rule has two shortcomings. First, the proposed rule does not establish a uniform, minimum standard for protecting the storage of personally identifiable information. Second, the proposed rule does not extend the security safeguards to implementations of the REAL ID Act.

1. Uniform Minimum Security Standards

The proposed rule does not propose an established security standard for states to follow. Without an established security standard to protect the storage of personally identifiable information, the implementation of the security standards will be inconsistent, and at worst, be ineffective in protecting personally identifiable information. The Comprehensive Security Plan required of each state should meet a minimal standard for acceptability; that standard should be documented, widely accepted, and readily applicable to the data management conditions the states encounter regularly.

Recommendation #1 - We recommend that the Final Rule set forth an explicit standard for security policies and procedures for states to follow.

2. Security Standards for the Card Itself

Because the REAL ID requirements include an identity card people will carry with them most of the time, the security safeguards to personal information need to be extended to the card itself, not confined only to the information management systems operated by the state agencies.

Recommendation #2 - The Final Rule should recommend specific steps to prevent unauthorized access to personal information on the card, including any contained in the machine-readable zone (MRZ).

3. Proposed Uniform Minimum Security Standards

The American Association of Motor Vehicle Administrators (AAMVA) has developed an information security program. The state departments of motor vehicles, through their commercial driver's licensing systems, already participate in this information security program protecting the confidentiality, integrity and availability of information for all aspects of program business, including information on customers and employees.

The AAMVA program, like most enterprise security programs, includes standard requirements for that could be included in the Comprehensive Security Plans and that address all of the following areas:

- System Access Control, allowing only authorized persons' access to data
- Computer and Operations Management, implementing practices to protect data and operational integrity
- System Development and Maintenance, developing procedures for protecting data security and privacy in coding, testing, and maintaining databases with personal information
- Physical and Environmental Security, providing safeguards protecting the locations, buildings, and areas containing the technology equipment and information resources
- Compliance, providing methods for monitoring and auditing compliance with requirements, as well as responding to suspected instances of non-compliance
- Personnel Security, implementing controls to assure that personnel are properly vetted for handling personal information systems

- Asset Classification and Control, developing and maintaining schema's that categorize information and physical assets and implementing security procedures, including data retention and destruction methods, according to the appropriate classification

AAMVA's information security program meets or exceeds these best practices and is flexible and not technology-specific. For these reasons, states can match the scale and scope of their security plans to their particular needs and resources.

These policies provide security standards that must be used when storing personally identifiable information in information systems and in compliant REAL ID cards themselves. Additionally, by using AAMVA's security program as a baseline standard, DHS can expect not only that the states will submit truly comprehensive plans, but will also have a uniform way to evaluate each state's proposed plan.

Recommendation #3 - The AAMVA information security program and standards should be the foundation for a comprehensive security standard that will be developed and defined by AAMVA working with the states and DHS, that will be published and applicable specifically to REAL ID implementations.

B. Privacy Safeguards

The Comprehensive Security Plan does not address critical privacy issues. The Committee recommends that the Comprehensive Security Plan address critical privacy issues. First, the plan should articulate required privacy safeguards to enforce accountability and provide methods for consumers to inquire or complain about the collection, storage, and use of personally identifiable information and remedies for errors. Second, the plan should notify consumers of information collection and use by the state, provide choice over secondary use of that information, facilitate access to personal information for correction, and assure consumers that the information collected for a specific purpose is used only for that purpose.

The committee recommends that the requirements for states to include privacy protections in their Comprehensive Security Plans should be explicitly stated and defined.

Accountability

Currently, the proposed rule does not make states accountable for the personal information they are required to collect. All policies, practices, and technologies supporting the privacy and security of personal information should be documented. Collecting, storing, and using personal information requires a duty of care for its protection and reasonable management. Responsibility for compliance should be assigned to specific individuals within the controlling organization.

Recommendation #4 - The Final Rule should require that states are accountable for the personal information they collect and store and should assign individual responsibility to carry out that duty.

Redress and Remedy

Implementing REAL ID nationwide demands complexity, coordination, and oversight. Despite everyone's best efforts, errors will occur and redress procedures will be necessary. The proposed rule does not contemplate such errors. To mitigate against the privacy erosive effect of such errors, procedures for responding to and redressing inquiries and complaints about the use of personal information should be widely available, easy-to-use, and staffed appropriately for prompt and accurate response. Liabilities for misuse of personal information, including sanctions, should be included in the policies for redress.

Recommendation #5 - The Final Rule should require that states include procedures for individuals to submit inquiries and/or complaints about compliance with stated collection, storage, use, sharing, and management of personal information in their Comprehensive Security Plans.

A number of other factors related to privacy also need to be considered when developing security guidance. DHS should evaluate the ways in which states give effect to the concepts of Notice, Consent, Access, and Limited Purpose. The Committee has set forth the criteria against which DHS should evaluate state practices, procedures, and implementation for their effectiveness and practicability. The evaluation process should also take account of the analysis framework previously developed by this Committee.

Notice

Currently, the proposed rule fails to require state agencies implementing REAL ID to provide notice to consumers about their information collection, storage, and uses of personally identifiable information. Privacy notices provide openness and transparency, which are vital components of a substantial privacy regime. Failure to provide openness and transparency undermines accountability and trust.

At a minimum, the privacy notices should include:

- Details of personal information collected
- Details of data processing verifying collected data, including the source data against which the collected data is verified
- Personal information stored, including the retention period
- Purposes for which information is collected, used, retained, and disclosed to others; specified purposes should be clear, limited and relevant
- Safeguards used to protect personal information from unauthorized access, use, or compromise
- Procedures by which individuals will be notified of changes to information management practices, including the ability to opt-out, as appropriate
- Methods employed to assure compliance with the stated practices such as monitoring, audits, and compliance verification
- Mechanisms for complaints and redress, including available processes for individuals to utilize

Recommendation #6 - When evaluating the Comprehensive Security plans, DHS should evaluate the privacy notices detailing information collection, storage, and use practices. These notices should be readily available to all individuals whose information is affected.

Consent

While individual consent is required for the collection, use or disclosure of certain types of personal information, unless otherwise required (or permitted) by law, a person may withhold consent simply by not participating. However, in the context of applications for driver's licenses, driving is an important privilege and often an economic necessity for most adults.

In the context of REAL ID implementations, consent is perhaps more meaningfully applied to uses of personal information OTHER than those primary uses explained in the privacy notice.

Recommendation #7 - When evaluating the Comprehensive Security plans, DHS should evaluate the opportunity to "opt-out" from secondary uses of personal information appropriately noticed in advance of the application for a driver's license. We believe an exception for law enforcement agencies would be appropriate.

Access

That individuals are able to review personal information held by others is a universally accepted privacy principle. This principle includes providing data subjects with the ability to question and to correct inaccuracies in personal information collected and stored by others. Currently, the proposed rule does not require states to provide that access and we recommend that it should be included.

Recommendation #8 - When evaluating the Comprehensive Security plans, DHS should evaluate individual access to sources of personal information. First, data subjects should have access to the information about themselves collected by their state agencies. Second, data subjects should be provided help in accessing the reference databases used for information verification.

Providing data subjects access to reference databases is particularly important for instances in which an individual application is rejected or fails because of verification issues. Because the states are not currently able to provide direct access to those databases operated by others used in verifying identity documents in applications, then at a minimum, they should be able to direct individuals to the responsible agency for data subject access.

Limited Purpose

Privacy is best protected when information collected for a specified purpose is used exclusively for that purpose. The proposed rule does not require states to implement controls that would limit the purpose for which information is collected and limit the use of that information to the stated purposes. Controls for limiting the purposes for which personal data are used require that all uses be consistent with those described in the notice provided at collection, that changes are subject to a documented review process, and that any individuals whose information was previously collected be notified of subsequent changes and provided choice for new uses, as appropriate.

Recommendation #9 - When evaluating the Comprehensive Security plans, DHS should evaluate inclusion of the principle of limited purpose including:

- **Restrictions on unilateral authority to change required uses for the REAL ID cards**
- **Restrictions on unauthorized uses, including commercial uses as a standard identifier**
- **Implementation of Notice & Consent options for any secondary uses, including requirements**

for consent for such uses

II. Storing Personal Information in the Machine Readable Zone

Many states already store personal information in machine-readable form on drivers' licenses. The committee recognizes the need for law enforcement officers to retrieve information quickly and accurately from a driver's license. However, we also recognize that the benefits of fast and accurate retrieval of this information are not limited to law enforcement. Commercial entities have already begun exploiting this low-cost retrieval process and are generally gathering more information than is needed for their purpose. To make things worse, there is the likelihood that certain data will be used beyond the limited purpose for which it was gathered.

There are two additional threats to the information stored in the MRZ. First, though encryption schemes could protect the data in the MRZ from unauthorized access, critics of encryption argue that proper implementation depends on managing encryption keys across the multiple jurisdictions, which is unlikely to be efficient or effective. Key management failings would result in a broken encryption schema.

Second, even if an encryption system could be effectively managed for the MRZ data, Optical Character Reader (OCR) devices could electronically read the personal information printed on the face of the card, thereby overcoming any protective benefits of encrypting MRZ data. This potential threat to the privacy of individual personal information might be mitigated by reducing the amount of personal information stored in the MRZ.

Recommendation #10 - We recommend that DHS re-evaluate the appropriateness of the proposed technology for the Machine Readable Technology. If the current approach is maintained, the Final Rule should require a reduction in the amount and the type of information stored in the MRZ to include:

- **Bearer's name and address**
- **Unique record identifier - not the license number, but used to look up the license number on the state system**
- **License issue and expiration date**

This information supports law enforcement's need for safety and identity requirements and is useful to detect forgeries and look up wants and warrants, yet reduces the useful information available to common commercial scanning scenarios.

III. States' Electronic Access to Other States' Driver's License Databases

The recommendations above, including standardized information security protections and recognized information privacy standards, are good protections for intra-state information management and protection. They are equally useful when states share information with other states, a necessary practice in reducing false

claims of identity, issuing multiple licenses to the same individual, and reporting specific legal conditions and behaviors necessary for public safety. Even with common security standards and the deployment of standard privacy protections, each state will have unique characteristics within their own internal policies and operations. To assure the appropriate enforcement of those policies and procedures when data is shared with entities outside the state's control, it is important that they be communicated along with the data.

Some possible solutions, including data coding procedures, are already widely deployed in the private sector. These procedures create constraints against unauthorized use when carried with the data itself. Employing meta-tag methods, the personal information can be marked with specific data classifications, use and sharing restrictions, retention periods, and other policy-driven constraints. By deploying tagged (or coded) data, each state would convey their own security and privacy principles whenever they share information with other states. This method of communicating the security safeguards and privacy protections for personal information, embedded with the data, is superior to off-line instructions.

In essence, having made privacy and security promises to the individual from whom it collected the information, the tagging scheme communicates those promises to everyone who has access to the data, greatly aiding compliance with the promised practices.

Recommendation #11 - The Final Rule should require that all state driver's license databases specify the restrictions on access, onward transfer, and secondary uses of personal information.

IV. Background Checks for Employees in Manufacturing and Production Facilities

With respect to performing background checks and keeping that information current, the final rule should impose obligations on DHS as well as on individual states. DHS and other federal government agencies are experts in conducting background checks on employees. Individual states may not have the resources (human and financial) or the experience in conducting, comprehensive security checks on each subject employee. Moreover, DHS has the capacity to conduct background searches and is already doing so through Strategic Threat Assessments in the air cargo industry. For example, earlier this year, DHS issued a final rule requiring certain persons related to Indirect Air Carriers to submit to DHS information as part of a Strategic Threat Assessment so that those persons could be cleared by DHS to work with Indirect Air Carriers. Because REAL ID envisions a "federated" system, with different parties playing different roles in partnership, we believe the federal government, through the DHS, is best positioned to provide resources and expertise in this area

Recommendation #12 - The Final Rule should specify that DHS conduct the initial background search of the subject employee in state facilities involved in the manufacture or production of REAL ID licenses. It should also require the states to use direct data feeds from federal agencies and even consumer reporting agencies to maintain the currency of the employee's information and allow states to maintain the employee clearance over time.