Association for Computing Machinery

Advancing Computing as a Science & Profession

Comments on Notice of Proposed Rulemaking
Minimum Standards for Driver's licenses and Identification Cards Acceptable by
Federal Agencies for Official Purposes
(Docket No. DHS-2006-0030
RIN 1601-AA37)

U.S. Public Policy Committee of the
Association for Computing Machinery (USACM)

May 8, 2007

On behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM), we are submitting the following comments on the Notice of Proposed Rulemaking (NPRM) for the REAL ID Act.

With over 80,000 members worldwide, the Association for Computing Machinery is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.

Introduction

The REAL ID Act and the Department of Homeland Security's (DHS) proposed rules for its implementation create significant new privacy, security, technical and societal issues. States will now be required to collect, digitally scan and retain personally identifiable information such as birth certificates, permanent resident cards, and U.S. passports. These documents will be kept in distributed databases, linked with the REAL ID issued to that person and spread over all 56 jurisdictions covered by this rule. Identity documents will need to be verified against numerous other databases from which they originated. Numerous officials, ranging from Federal and state law enforcement officers to local Department of Motor Vehicle (DMV) workers will have access to all of this information both within and outside their jurisdictions. This entire system will be required to operate smoothly, issuing and maintaining REAL IDs for the approximately 240 million drivers licenses and identity cards currently in circulation, while at the same time protecting the privacy of individuals and ensuring accuracy across databases and information sources that are notoriously inaccurate. These are daunting challenges that depend on the proper policy framework for protecting privacy, ensuring security, and maintaining the accuracy of personal information.

In our view, these proposed regulations fall far short of meeting these goals for two reasons: First, the underlying policy embodied in the REAL ID Act is flawed. Second, the NPRM fails to set clear minimum standards for states to follow. The Real ID Act establishes as a national policy a de facto national identification system by requiring states to collect, maintain, and share vast amounts of personal information and issue standard identification to all Americans, but the law does not speak to privacy, security or accuracy concerns. The proposed NPRM does not address these shortcomings by expressing strong protections, standards or detailed guidance.

The NPRM notes several times that states will need to develop agreements to deal with state-to-state data exchanges, to create mechanisms for openness, and to submit “written, comprehensive, security plans.” However, it does not specify minimum privacy, security and accuracy standards that should be a part of these agreements or plans, nor does it create appropriate accountability for following these plans, or sanctions for violating them. These undefined requirements leave our committee concerned that as states are struggling to deal with the staggering costs of implementing the REAL ID Act while maintaining their current levels of service, they will devote minimal resources to protecting the elements of what they implement.

The NPRM is also silent on issues of accuracy. If implemented as written, the REAL ID system will connect several different databases to check a REAL ID's status and verify documents. It also relies on several different kinds of documents to demonstrate a person's identity, place of residence, and other criteria. There are no procedures in place to handle data entry mistakes, differences in names, the inclusion of middle names in some databases and not in others, and similar mismatches.

Because the REAL ID specifies a certain list of authorized documents to determine one's identity, people who are unable to produce these documents (or certified copies) will not be able to obtain REAL IDs. Without appropriate processes for reconciling errors or dealing with an absence of official documents, too many individuals will be inappropriately prevented from obtaining a REAL ID and the benefits associated with it.

We understand that the Department must promulgate rules within the limits of the underlying law. It is clear that the Department recognizes the flawed policy by stating that the previous law calling for stronger national ID standards, the Intelligence Reform and Terrorism Prevention Act (IRTPA), had stronger privacy and security protections[1]. Given the issues the law and the NPRM raise, we would rather see the Administration seek amendments to the law to deal with these issues, rather than push forward a flawed rulemaking. Ultimately, REAL ID provides an identity document that increases the risk of identity theft, exposes more personal data, and is a greater target for fraud and abuse.

REAL ID and Identity Theft

The NPRM, and comments from DHS staff, have suggested that REAL ID will reduce the incidence of identity theft. The apparent bases for the claim are the increased scrutiny of documents under REAL ID and the improved security of the REAL ID itself. Our

[1] NPRM, page 10825, footnote 3, "The [Real ID] Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act. This is in sharp contrast with the express authorization provided in section 7212 of IRTPA, which was the prior state licensing provision repealed by the Real ID Act. Section 7212(b)(3)(E) of IRTPA stated that the Federal regulations "shall include procedures and requirements to protect the privacy rights of individuals who apply for and hold driver's licenses and personal identification cards."

detailed comments raise serious security questions about the proposed implementation of REAL ID. Those questions suggest that the document will not be as secure as the DHS claims, undercutting the notion that the REAL ID will decrease the incidence of identity theft. A more fundamental problem, however, results from the DHS perspective on identity theft.

Theft of driver's licenses (or identification cards) and related documents is not the predominant form of identity theft today. Most identity theft is conducted to exploit the credit histories of the victims rather than to impersonate an individual with the intent to commit crimes under an assumed identity. Social Security numbers and credit card numbers are the usual targets of this form of identity theft. REAL ID does little, if anything, to reduce this. However, by presenting the REAL ID as a “gold standard” identification document, the NPRM risks encouraging a different form of identity theft: one where people will assume someone else's identity and conduct criminal acts as that individual. This increases the incentive to forge a REAL ID or to buy a valid REAL ID from a dishonest insider, because the REAL ID is more valuable to those seeking to commit criminal acts.

An identity stolen through a forged, stolen, altered or fraudulently-obtained REAL ID will be much harder to recover. Victims of identity theft already have a great struggle to restore their identities and to clear their name from credit fraud or criminal charges for which they are not actually responsible. When a REAL ID is compromised, the underlying data is also at risk, and because there is much more data supporting a REAL ID, there is much more data to reclaim, and that much more work for the victim.

To minimize the damage of potential identity theft, the identifier number on the REAL ID should:

- not contain or be based on information that could be associated with the individual (such as a partial or full birth date or a Social Security number); and
- not be associated with that individual in any other documents or databases, but only with that particular REAL ID card.

That way, if the card is reported stolen, the identity can be disconnected from the identifier, minimizing the damage of identity theft for the victim and the damage the thief could do with a stolen REAL ID.

A similar practice is used in the credit card industry, where a company replaces a lost or stolen credit card with new card containing a different number. When a person notifies a credit card provider that a card is lost or stolen, it does not result in a new customer file, but rather a new card with a different number. The number of the lost or stolen card is deactivated and/or noted as lost or stolen. A similar practice with REAL IDs would minimize the damage caused by an identity thief using a lost or stolen card.

Insider Threats

The NPRM is silent with respect to insider threats to security. This is the most likely way that an individual's identity will be stolen. For example, an official with access to data required by the act steals personal information for wholesale identity fraud, or someone with the authority to issue REAL IDs accepts fraudulent documents to create authentic REAL IDs. The Federal Trade Commission Identity Theft Survey Report[2] notes that individuals in businesses or agencies with access to personal information facilitate a significant percentage of identity theft. This is a threat under the existing driver's license system[3], but the REAL ID Act makes the problem far worse. It vastly increases the amount of personal information stored, and therefore potentially exposed, on state databases and the value of the identity card.

[2] http://www.ftc.gov/os/2003/09/synovatereport.pdf

[3] For example, a Maryland MVA employee was charged with conspiring with others to sell more than 150 state identification cards. See Eric Rich, 2005, "MD, MVA Employee Charged in ID Card Sales," *Washington Post*, April 23, p. B03. For a collection of stories of security problems of motor vehicle records, see Center for Democracy and Technology, *Tracking Security at State Motor Vehicle Offices*, available online at http://www.cdt.org/privacy/030131motorvehicle.shtml.

Minimum Standards and Clear Definitions

The NPRM should establish minimum standards for privacy, security and accuracy of REAL ID documents. As written, it is at best suggestive that the states and agencies that implement the law should have security standards and privacy protection, but vague on the details. Given the number of recent data breaches in all sectors of society, including agencies that will issue the REAL IDs and store documents and data, best efforts to address security, privacy and accuracy concerns are needed. The NPRM places much more information in electronic databases and in storage at DMVs than previously held, and thus must require a set of security and privacy standards to minimize the occurrence of breaches and mitigate the damage caused by them.[4] Concerns for security and privacy are not mutually exclusive – they are inextricably linked. Proper privacy protection can help ensure a more secure system, both in minimizing risk and increasing the ability to detect breaches, and proper security is fundamental to ensuring privacy.

The NPRM makes reference to fair information practices, but does not define them. Fair Information Practices (FIPs) [5] have a history of providing guidelines for the protection of privacy rights. Explicitly incorporating FIPs in the NPRM can go a long way toward alleviating concerns that people have about the impact of REAL ID on their privacy. We strongly suggest the NPRM embrace standards similar to those of USACM's privacy principles[6], including the following basic provisions:

Minimization – If the use of REAL ID is expanded beyond current law, collect only the data that is absolutely necessary for those purposes, and keep it for only as long as necessary. Periodically review and remove information once the required time periods for storage have ended. This would apply to the information on the front of the license or identification card, data stored in the machine-readable zone (MRZ), and the documents and information used to apply for or renew the REAL ID. Procedures for storing REAL

[4] Breaches reported at the Oregon and Georgia motor vehicle departments in 2005 exposed the information of over 600,000 people.

[5] Consult http://www3.ftc.gov/reports/privacy3/fairinfo.htm for more information

[6] USACM's privacy principles can be found at http://www.acm.org/usacm/Issues/Privacy.htm

ID information for deceased persons or those who have moved to another jurisdiction should minimize the data stored, both in terms of quantity of data and locations where it is stored.

Consent – The collection or sharing of information about an individual needs to be explicitly explained to REAL ID applicants. To the extent allowed by law, inform applicants about the extent of collection and sharing of their personal information, both when it is first collected, and also for any additional use ("other purposes" under the NPRM) determined after the information is initially collected. Informing people about the use and sharing of REAL ID data, and allowing them the option to give or withhold their consent helps make clear the consequences of REAL ID use.

Openness – Explicitly and clearly communicate the precise purpose for the collection and use of the information and how long it will be stored. This applies to any current uses of the REAL ID, and any new or additional uses for the REAL ID.

Access – Provide individuals with tools for accessing the information stored for the REAL ID, and for requesting revision or correction as needed. For instance, if a person's name is misspelled on a Social Security card, that person needs to be able to review the material and request a correction. Access should include a record of any parties with which the information was shared, so people can request corrections by those parties as well.

Accuracy – Develop and publicize a process for handling inexact matches and mismatches of names and information stored for REAL ID. Inaccurate information undercuts the value of the databases and the REAL IDs that depend on them. Databases used for REAL IDs need to be checked regularly by those agencies and individuals responsible for their operation, with any updates propagated to all of the related databases and institutions. For example, if a birth certificate in the Electronic Verification of Vital Events (EVVE) database is found to be fraudulent, there needs to be a way to communicate that error to all REAL ID licensing agencies. Upon notification, they can deactivate the REAL ID based on that birth certificate and prevent that document from being used to apply for another REAL ID.

Uniformity of practice will help make sure data is entered consistently across databases, reducing the incidence of mismatches and false positives or negatives. This applies to the MRZ data as well as the databases used to confirm identity. If state A kept information on the front of the license and in the MRZ that state B did not, there could be a problem when a citizen of state B has their REAL ID checked in state A. Not seeing any information for the field state A keeps information on (but state B does not) may prompt a law enforcement official to assume action or intent unwarranted by the fact that state B does not collect such information.

Security – Implement security measures that incorporate all reasonable and appropriate physical, administrative and technical measures to maintain the confidentiality, integrity, and accuracy (CIA) of all potential storage and transmission of the data, in any form. This includes information on the REAL ID as well as the information stored in related databases or with the relevant DMVs. With REAL ID and this NPRM, there are several important questions regarding access to data, which we will discuss below.

While the NPRM and the act address concerns over physical security, they are relatively silent on computer security guidelines. Given the increase in electronic records storage and transmission under the REAL ID, we urge the Department to adopt computer security standards. We suggest standards that would meet the recommendations for configuration and management of information systems as developed by NIST. Additional standards that could be considered include those published by the ISO (International Standards Organization), and the Common Criteria Evaluation and Validation Scheme (CCEVS). The CCEVS is managed by the National Security Agency, and participating laboratories are accredited through the National Institute of Standards and Technology's NVLAP – National Voluntary Laboratory Accreditation Program.

Accountability – Use a variety of methods – including audit logs, internal review, independent audits and sanctions – to ensure compliance with privacy policies. Provide training and tools for maintaining provenance on the data for at least as long as it is stored. There need to be sanctions for failure to maintain data privacy and security. This issue is critical enough that the Administration should ask Congress for sufficient authority in this area to ensure accountability if they do not believe that have it under the existing law. The regular security audits required by the FTC in proceedings such as the ChoicePoint settlement are an example of a best practice that must be implemented for REAL ID.

These principles would take the NPRM a long way toward increasing privacy protection, data security and accuracy of personal information. Ensuring a minimum standard would benefit the entire system by requiring these protections, rather than simply hoping they will be implemented.

Access Controls

There is no guidance in the NPRM on who is allowed to access REAL ID information, whether it is via the MRZ, the local DMV, the databases that support the REAL ID system, or the proposed federated query system for these databases. Such standards need to be developed and publicized to assure the public that their information will be safeguarded. A lack of transparency in the access to electronic voting machines has gone a long way in undermining public confidence in that technology – a process that could easily be repeated here. If left to the states, we envision a scenario where there is a multitude of standards for privacy and security, and the jurisdiction with the weakest standards will be a prime target for those seeking to defraud the REAL ID system.

A system of access controls that determines who has what level of access (read-only, write, administrative and execution) supports many of the recommendations we make in our comments, particularly the minimization, security and access principles we describe above. Access control policies should minimize the number of people who receive privileges either to access each piece of information or to grant access to others. They should also ensure that each person is granted only the minimal set of privileges needed to do his or her job. Following these guidelines can provide significant protection.

Access controls determine who is allowed to access what data and what level of access they should have. Read-only and write access categories are straightforward. There should also be an administrative category – where the person with administrative access would have the authority to specify what access other people have. This could be on a state, regional or national system, depending on whether we are dealing with DMV data or federated query service data. A final category of access control is execution access – or functional access. This would specify what functions a person could perform.

Users will need to be authenticated every time they access the system, at a minimum. It may be prudent, depending on the information being accessed, for users to be authenticated any time they access particular information or documents, much like a cashier must input his access code to activate his register. This information should be recorded with non-volatile logging to provide a robust audit trail to be used in cases of misbehavior.

Users should be given differing levels of access based on the actions they must perform. Further, users should not be given more rights than they need to do their job. Restricting access helps minimize the risk of data breaches, whether accidental, intentional or by inside threat. Access needs to be restricted in terms of how many people can read or write data and how much data they can access. For example, a clerk may have read-only access for all entries at their DMV, but write access only for a certain range of files. Access to multiple-state data could be restricted to individuals responsible for the federated query search. This helps ensure accountability by better linking data responsibility to specific individuals.

We emphasize the need to be clear and explicit about who can and cannot access the information available on a REAL ID, as well as who can and cannot access the databases and documents used to support this system. Such a large collection of data is a ripe target, not only for theft and abuse, but also for third parties to accumulate data in a relatively inexpensive manner. If third parties start requesting that customers present the ID so they can access the information and use it for their private purposes, multiple national commercial databases are likely to be established, without any form of regulation. The most effective means of limiting such access would be to minimize the data stored on the MRZ, and carefully spell out access requirements for the REAL ID, the query service, and associated databases. Sanctions for violating these standards, and for harvesting information without an individual's knowledge and consent, are needed to deter people from attempting to use this wealth of information for reasons that have nothing to do with security or with the other stated purposes of the act. Without sufficient deterrence, everyone's privacy is at risk.

We strongly recommend that access control guidelines be included as part of the states' plans for compliance with REAL ID.

A National Database

The NPRM notes that neither the law nor the NPRM establishes a national ID; however, the limited security and privacy standards and lack of access controls will make it relatively easy to create a national ID database from REAL ID data. Individual DMV workers, burdened by limited resources and a public demanding quick service, may place other aspects of job performance above security, increasing the risk of data breaches. Such exposure allows for the collection of information on people in that state and people with documents stored at that state DMV. Third party vendors, whether contracted to state DMVs or collecting IDs for other purposes, will collect the information or sell it to other parties interested in a national database. A national database can be compiled through determined skimming of the MRZ or through lax security practices in only one office of one of the participating jurisdictions. Privacy interests need to be protected from intrusions by other parties as much as by the government. Without minimum standards for privacy, security and access, we are at risk of other parties creating a national database.

The NPRM fails to give any specifics about the federated query service that would check for duplicate registrations in other jurisdictions. Without guidance from the government, it is uncertain that any strong security and privacy standards with this service will be developed or implemented. One reason the DHS maintains that the REAL ID will not be a national ID or become a national database is that the federated query service will simply check for the registration status of an applicant in any other REAL ID compliant jurisdiction. This would involve a simple yes/no query of the relevant databases. However, given the mobility of most Americans, in the application and/or renewal process for a REAL ID one DMV will need to consult with other DMVs not only about the existence of other REAL IDs, but about the authenticating documents that may be stored at those DMVs. This requires much more than a simple yes/no query. If the DMV must verify the identity of a renewal or relocated applicant, it will not be enough to simply check if she has a birth certificate (or other document) on file in another jurisdiction. They will have to verify that document – they will have to link to that database. Their need to do so will place pressure to create a *de facto* national database that supports a *de facto* national ID system.

Premature Implementation

Several of the databases described in the NPRM are still in development or are not fully operational. While DHS has received assurances that at least one of these systems – the Electronic Verification of Vital Events database – could be ready by the NPRM's May 11, 2008 deadline for state implementation of REAL ID, it seems likely that not all of the necessary databases will be operational by the time states must start issuing REAL IDs. While the NPRM does not discuss what would happen in this event, we anticipate the burden being shifted to the states – much as it has with respect to the monetary and personnel resources required to implement these rules. In short, until these databases are operational, DMV staff will be required to collect a greater amount of information per person, verify that the documents presented are authentic, and handle the increased traffic of individuals who need a REAL ID card and would have otherwise not needed to visit the DMV, or would have renewed online.

USACM has followed the adoption of electronic voting machines over the last several years, and noted the challenges states and localities faced when encouraged to adopt new technologies in a short time frame, with limited federal support, relatively new technologies, and no new standards prior to deployment. The resulting struggles and mistrust could happen again with overburdened DMVs, dissatisfied customers, many people opting out of the REAL ID or, as we have already seen, states passing legislation to opt out of the system to avoid the inconvenience and threats to privacy. A significant increase in the number of people or states choosing to forego having a Real ID would undermine the intent of the act.

We have seen a pattern from other instances of large municipal programs with hard deadlines and complex IT requirements. As the deadline approaches, there is a push to make the IT systems operational. Last minute decisions are made to use a system that has not been fully tested, or whose features have not all been implemented (or both). The result is almost always disastrous. Setting a hard deadline that will be difficult or impossible to meet for REAL ID may well result in going "live" with systems that are missing security and privacy features, that lose or corrupt data, and that fail to meet basic requirements. As a result of enforcing unrealistic deadlines, there could be major problems following deployment of the REAL ID systems before the entire federated system has been thoroughly tested.

Delaying implementation until testing is completed will reduce future problems with the implementation and operation of REAL ID. It will also reduce the considerable costs of the system. We recommend that REAL ID implementation be delayed until all of the underlying databases have been fully tested against established benchmarks and are operational.

Data Breach Notification

The increased amount of data involved with the REAL ID – both electronically and at DMV facilities – increases the risk of data breaches, even if security, privacy, and access controls have been implemented to protect the system. Strong sanctions for violations of procedures are required to deter the insider threat. Additionally, everyone whose information is exposed in a breach needs to be notified of the breach so as to watch for possible identity theft. To that end, we recommend that data breach notification be required for the REAL ID. The California law on data breach notification is a useful model in this area. Current legislation being considered for national data breach notification would be worth examining as well. We encourage DHS to review USACM's detailed comments on what breach notification standards should be part of the federal legislative efforts.[7]

Specific Questions

We now address some of the questions noted in pages 92-96 of the NPRM. The questions are in *italics*.

(1) *Whether the list of documents acceptable for establishing identity should be expanded. Commenters who believe the list should be expanded should include reasons for the expansion and how DMVs will be able to verify electronically with issuing agencies the authenticity and validity of these documents.*

We recommend not expanding the list of documents. Despite the ease it may provide people in demonstrating identity, these additional documents must be verified, either through databases or individual examination (or both). That will place a burden to verify the additional documents on licensing agencies and those bodies responsible for databases. Every individual examiner will need to become familiar with more kinds of

[7] http://www.acm.org/usacm/weblog/wp-content/USACM_comment_House_EC_bill_final.pdf

documents that they may see in their work. Their judgment and workload will determine whether inauthentic documents are mistakenly accepted, and whether some legitimate documents are mistakenly rejected. Many more databases will need to be checked, and the information in those databases must be reviewed for accuracy, double entries, slight name mismatches, and other data issues. Further, expanding the list of document would expand the amount of personally identifiable information stored on state databases, which would increase privacy risks.

(2) *Whether the data elements currently proposed for inclusion in the machine readable zone of the driver's license or identification card should be reduced or expanded; whether the data in the machine-readable portion of the card should be encrypted for privacy reasons to protect the data from being harvested by third parties, and whether encryption would have any effect on law enforcement's ability to quickly read the data and identify the individual interdicted. What would it cost to build and manage the necessary information technology infrastructure for State and Federal law enforcement agencies to be able to access the information on the machine readable zone if the data were encrypted?*

Given the widespread availability of readers for the PDF 417 standard, the ability to read the bar code through other means[8], and the storage capacity of the bar code standard, encryption could help protect the security of the document and the privacy of the document holder. However, given the number of agencies and law enforcement personnel who would need to access the MRZ, the number of readers containing the key(s) necessary to preserve encryption and allow for cross-jurisdiction access is significantly large. Keys would have to be "frozen" when each REAL ID document is created. It would impossible to change the keys when they are inevitably leaked (as has happened with DVDs) without invalidating and reissuing the impacted IDs. The impracticality of an effective key management protection scheme reinforces the need to minimize the data stored on the MRZ. This would minimize the data that could be exposed, mitigating (but not eliminating) the privacy and security risks of unencrypted

[8] For example, taking a picture of the MRZ and then later decoding the information.

data. Such minimization must be coupled with strong access controls and data breach notification procedures in the event that REAL ID information is exposed.

To reduce the risk of identity theft, we strongly recommend that any MRZ data should be restricted to no more than the information on the front of the license or identification card.

(4) *If a State chooses to produce driver's licenses and identification cards that are WHTI (Western Hemisphere Travel Initiative)-compliant, whether citizenship could be denoted either on the face or machine-readable portion of the driver's license or identification card, and more generally on the procedures and business processes a State DMV could adopt in order to issue a Real ID driver's license or identification card that also included citizenship information for WHTI compliance. DHS also invites comments on how States would or could incorporate a separate WHTI-compliant technology, such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF417 barcode requirement.*

While RFID may make it easier to scan data, it poses a greater risk for skimming than even an unencrypted MRZ. If RFID were to be used, any encryption scheme has the same risks described above with respect to the MRZ. The ability to passively skim information from an RFID chip makes it a poor technology for ensuring privacy and security.

Furthermore, the WHTI information should be kept separate from the REAL ID information. The WHTI requires different information than the REAL ID, and serves different purposes. By mixing the data, it becomes easier to gather information not relevant to the official purposes of each program. Further, other countries and international agencies will access the WHTI information, and they have no compelling interest in the REAL ID information.

While documents used for the REAL ID can demonstrate citizenship and/or lawful status, making this a more explicit part of the identity document makes the REAL ID a two-tiered system based on citizenship. Clear markers of citizenship can encourage theft or sale of these documents by those seeking to fraudulently demonstrate citizenship status. Additional purposes for the REAL ID increase the risk of failure for the stated purposes.

***(5)** How DHS can tailor the address of principal residence requirement to provide for the security of classes of individuals such as federal judges and law enforcement officers.*

To minimize the exposure of addresses for certain classes of individuals, address data could be stored solely on the MRZ. However, use of the PDF417 standard enables software and readers to extract the data from a photograph of an unencrypted bar code. The number of different groups that may need to access the MRZ, and the need to hard-wire an encryption key into the identification card makes effective encryption management impractical at best. This increases the need for appropriate access controls, sanctions for violating those controls, and data breach notification requirements to protect REAL ID holders.

A better level of protection would be to note in the MRZ that the individual's address is protected and provide a pointer to whatever relevant authority handles these addresses for their jurisdiction. This would also serve a secondary purpose: anyone seeking the address would make a request that could be logged and validated, thus further preserving the privacy and security of the persons with restricted addresses.

***(11)** How the Federal government can better assist States in verifying information against Federal databases.*

The Federal government should establish and publicize processes for individuals to review and correct the data already in the various databases that will be used for REAL ID. Ensuring accurate information is a good first step toward improving verification of that information. The Federal government can also establish minimum guidelines for the security, privacy and accuracy of its databases and whatever means are used to access these databases.

***(14)** Whether other federal activities should be included in the scope of "official purpose."*

We oppose any expansion of the official purposes of the REAL ID. Additional purposes increase the exposure of information on the document, and may well increase the amount of information stored on the document. Any increase in the official purposes of the act must be accompanied by public notice of what purposes the information will be used for, and any additional data that will be collected and stored, per the privacy considerations addressed earlier in our comments.

If the other federal activities considered here would involve additional data, it is important to consider the additional burden on state agencies and the privacy of individuals. Will the agencies need to store additional data and verify additional documents? Will the federated query service need to check additional databases? Given the scale and complexity of this system, making changes to it will also incur significant costs. All of the questions raised about the initial system must be re-answered, and tests completed, prior to enactment of any expansion.

Any expansion of official purposes that requires an increase of data stored on the MRZ compounds the privacy and security risks to REAL ID holders. Given the number of law enforcement agents (and others, depending on the new official purpose(s)) who may need to access the MRZ, and the hard-wired key required for the ID card, effective encryption is impractical. Minimizing the official purposes of the REAL ID is one way to limit the risk of data breach or misuse.

There is often a mistaken belief that authenticated identify is sufficient to determine motivation. Experience has shown that this is not the case. Further, every criminal and terrorist has an identity, and none have a criminal history before their first criminal act.

The use of the REAL ID as a measure of security is usually questionable, and any additional uses for this purpose should not be allowed.

There are also likely to be many people who are either unable or unwilling to produce the documents required to obtain a REAL ID compliant license or ID card. Many or most of these individuals will be law-abiding residents of the U.S. Any additional uses of the REAL ID would deny those persons benefits, access or equal treatment without due process of law.

(15) *How the REAL ID Act can be leveraged to promote the concept of "one driver, one record, one record of jurisdiction" and prevent the issuance of multiple driver's licenses.*

The privacy, security and accuracy of the underlying information will help ensure that one person holds only one valid REAL ID at a time. The privacy and security principles we emphasize earlier in the document will make the databases, and by extension the document, more private, secure, and accurate.

The federated query system is critical in ensuring this policy goal. It must be well developed and tested. If it suffers from failures, whether they are false positives, false negatives, or an inability to handle the load, the chance increases that the service will be circumvented, undercutting the reliability of checks for duplicate REAL IDs. One of the proposed models, the Commercial Drivers License Information System, or CDLIS, does an effective job for the commercial drivers license registration system. However, there are two differences worth noting. First, it is not a federated query service, but a national database. Simply scaling up this system will not establish a federated query service, but will create a national ID. Secondly, CDLIS handles a much smaller collection of records than the estimated 240 million needed for full implementation of REAL ID. A system that works well on a small scale often needs to be re-designed, and still needs to be tested, when expanded to handle a much larger load.

It is unclear from the NPRM how the federated query service will operate and manage the data between databases and DMVs. How would the federated query service handle corrections to data? Would data be duplicated in other databases connected through the query service? Does the service deactivate the previous REAL ID if one is found, or merely notify the other DMV? What happens to the documents stored at the other jurisdiction? Are they transferred? As some are digitally stored, are those documents kept at both jurisdictions? Strict access controls to REAL ID data and documents will help minimize security and privacy risks. Such controls will not be possible without answering these questions prior to implementing REAL ID.

(16) *Whether DHS should standardize the unique design or color required for non-REAL ID under the REAL ID Act for ease of nationwide recognition, and whether DHS should also implement a standardized design or color for REAL ID licenses.*

Such standardization makes REAL IDs easier for identity thieves to spot. It would also suggest to people that the REAL ID is a national ID, or at the very least part of a tiered ID system. In other words, a clear visual identification that a license or identification card is (or is not) a REAL ID increases the perception that a REAL ID is a national ID. This will prompt some people to consider the tradeoffs presented by REAL ID as described in the NPRM. Is opting out of a national ID worth the bother of not getting into federal facilities or on aircraft? Is choosing not to carry a license or identification card that is more likely to attract identity thieves worth the likely stigma attached to non-REAL IDs by the federal government and law enforcement? How people answer questions like these will affect how many people actually apply for a REAL ID.

However, persons checking IDs at airports and federal facilities need to be able to know that a license or identification card is a REAL ID, or a major intent of the law is undercut. One way to address this would be to identify the REAL ID only through the MRZ. The ID could then be scanned and identified as a REAL ID only when necessary to fulfill the official purposes of the act. While the impracticality of encryption makes it possible to identify a REAL ID with OCR software, it would be more difficult for criminals to spot a mark in the MRZ than a visible mark on the front of the license or identification card.

RECOMMENDATIONS

At a minimum, the final rule should require stronger, more detailed privacy, security and accuracy provisions than the NPRM. Even with the improvements to the proposed rulemaking we suggest below, existing technology and approaches cannot solve the policy problems raised by the REAL ID Act. We urge the Administration to send Congress proposed legislation to address these issues and frame the policy around privacy, security and accuracy goals – or to repeal the REAL ID act entirely. These issues should be addressed before the REAL ID Act becomes active.

1) Delay implementation of the REAL ID until all underlying databases and the federated query service have been fully tested and are operational. The experiences of the election boards that implemented electronic voting systems before standards and testing procedures were put in place demonstrate the folly (and increased costs) of implementing new technologies that are not thoroughly tested.

2) Minimize the data stored on the machine-readable zone (MRZ). With the possible exception of some notation that the ID is a REAL ID, and perhaps citizenship information, the MRZ information should be restricted to information on the front of the license or identification card. The difficulty of establishing strong encryption that allows appropriate access for law enforcement personnel and other agencies makes minimization of data in the MRZ even more important to minimize the data that could be skimmed or collected and used by other parties for unintended purposes.

3) Specify privacy, security and accuracy standards for the licenses, the databases, and the federated query service. Individual states may be free to implement additional protections, but a standard is essential, otherwise the state with the weakest standards places residents of all the other jurisdictions at risk.

4) **Base the privacy standards on the Fair Information Practices.** Fair Information Practices (FIPs) are a cornerstone of modern privacy practice, and should be familiar to the many vendors and agencies involved in REAL ID implementation. These provisions must include considerations of Minimization, Consent, Openness, Access, Accuracy, Security and Accountability, as we note in USACM's Privacy Recommendations (http://www.acm.org/usacm/Issues/Privacy.htm).

5) **Require security consistent with standards such as the Common Criteria Evaluation and Validation Scheme (CCEVS).** In addition to the physical security considerations of the NPRM, the Department must provide minimum computer, database and network security standards to the states.

6) **Include strong access control procedures for REAL ID documents and data.** It is critical databases follow strict access controls for who has access to what data, and how much data a person can access at one time. Such controls must include sanctions for violations and include recording with non-volatile logging to provide a robust audit trail to be used in cases of misbehavior

7) **Require data breach notification procedures for any agency controlling REAL ID data or documents.** The California state law requiring companies to notify their customers if personal information is exposed would be a good model for REAL ID data or documents. Similar legislation being considered by Congress would be another strong model.

8) **Limit the scope of the usage of REAL ID to only the uses specified by law.** We oppose any expansion of the official purposes of the REAL ID. Additional purposes increase the exposure of information on the document, and may well increase the amount of information stored on the document. Any increase in the official purposes of the act must be accompanied by public notice of what purposes the information will be used for,

and any additional data that will be collected and stored, per the privacy considerations addressed earlier in our comments.