CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

May 8, 2007

Secretary Michael Chertoff
Department of Homeland Security
Attn: NAC 1-12037
Washington, DC 20528

Re: **Comments on *Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (REAL ID Act)**
Docket No. DHS-2006-0030
6 CFR Part 37
RIN 1601-AA37

Dear Secretary Chertoff:

The Center for Democracy & Technology (CDT) appreciates the opportunity to provide comments on the Department of Homeland Security's proposed regulations to implement the REAL ID Act.[1]

CDT is a 501(c)(3) non-profit public policy organization dedicated to promoting the democratic potential of the open, decentralized, global Internet and related information technologies. Our mission is to develop and promote public policies to preserve and enhance free expression, privacy, open access, and other democratic values.

CDT has been a leading voice on privacy issues raised by identity technologies and by driver's license systems in particular. CDT was a member of the Negotiated Rulemaking Committee convened pursuant to §7212 of the Intelligence Reform and Terrorism Prevention Act of 2004[2] before that section was repealed by the REAL ID Act.[3] In 2004, CDT highlighted the

[1] *Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10820 (2007) (to be codified at 6 CFR Part 37) (proposed March 9, 2007) ("Notice of Proposed Rulemaking" or "NPRM").

[2] Intelligence Reform and Terrorism Prevention Act of 2004 [S. 2845] Pub. L. No. 108-458, §7212, 118 Stat. 3827 (Dec. 17, 2004).

problem of insider DMV fraud in a study entitled "Unlicensed Fraud: How Bribery and Lax Security at State Motor Vehicle Offices Nationwide Lead to Identity Theft and Illegal Driver's Licenses."[4] CDT recently submitted comments on the WHTI (Western Hemisphere Travel Initiative) PASS Card, a travel document proposed by the Departments of State and Homeland Security that would include a highly insecure RFID chip without clear practical benefits.[5]

I. INTRODUCTION

CDT's comments focus on the proposed regulations' implications for personal privacy and security. CDT recognizes that the REAL ID Act does not mention privacy and it barely mentions security.[6] DHS acknowledged this shortcoming in the Preamble to the proposed regulations: "DHS has sought to address these privacy concerns within the limits of its authority under the Act . . . DHS has sought in the NPRM to provide for appropriate privacy and security protections to the extent of its authority."[7] However, we disagree with the Department's conclusion that the lack of clear privacy and security guidance in the law precluded it from providing strong protection in the regulations.

While the Preamble includes an extensive discussion on privacy, the proposed regulations themselves fail to provide clear and comprehensive privacy and security protections. DHS did take some minimal steps to address the privacy and security of personal information held under the Act, but could have done much more on these key issues even under the statutory language as it currently stands.

CDT has long supported making both the issuance of driver's licenses and ID cards and the cards themselves more secure so that a driver's license or ID card will be a more reliable proof of someone's identity. However, such reform cannot happen without co-existent, meaningful privacy and security protections built into the program from the beginning.

CDT urges the Department to substantially revise the regulations to include significantly more privacy and security provisions. Privacy and security issues must be fully addressed in the implementing regulations; they cannot be deferred to being worked out as implementation proceeds. If DHS concludes that it does not have a sufficient record at this point to fully address privacy and security, then it should delay implementation and issue a *second* Notice of Proposed Rulemaking to set forth its tentative plans and solicit meaningful public comments.

[3] REAL ID Act of 2005 [H.R. 1268] Pub. L. No 109-13, Title II, §206, 119 Stat. 302 (May 11, 2005).

[4] <http://www.cdt.org/privacy/20040200dmv.pdf>.

[5] <http://www.cdt.org/security/20070108passcard.pdf>.

[6] CDT submitted written testimony to the DHS Data Privacy and Integrity Advisory Committee for its meeting on March 21, 2007 < http://www.cdt.org/testimony/20070321dhstestimony.pdf>.

[7] NPRM, Preamble at 10824-25.

CDT also encourages DHS to seek statutory changes from Congress to clarify the Department's authority to fully address privacy and security in its regulations, so that truly effective driver's license/ID card reform can be achieved.

Immediately below (Part II) is a summary of CDT's main recommendations to the Department of Homeland Security on how DHS can revise the final REAL ID Act rules to properly address privacy and security. Additional and more detailed recommendations and comments are included in the body of the document (Part III).

II. SUMMARY

1. Ensure that REAL ID Does Not Result in the Creation of a Centralized ID System

- While it is valid to ensure that a state DMV can determine whether a REAL ID applicant already holds a card from another state, the communication among the states should be accomplished in a way that does not create a centralized, national system of ID information.
- DHS should direct the states to develop a decentralized querying system and should reject the commercial driver's license system or other centralized system as the means by which states check with each other to determine whether an applicant already holds a license from another state.
- The final regulations should lay out in detail the architecture of the system that states will use to check with all other states to determine if any state has already issued a REAL ID driver's license or identification card to the applicant. This issue is too important to leave for resolution after the regulations are finalized.

2. Address Privacy And Security of Personal Data Stored In Databases and Shared Across Networks

- The final regulations should include specific minimum privacy and security standards for both state DMVs and federal agencies participating in the REAL ID system. These standards should address key privacy questions: What personal information may be collected and accessed, by whom, and for what purposes?
- The final regulations should limit access to and use of REAL ID personal information, including source documents, to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. This includes accessing cardholders' personal information directly from a state DMV database or via a national network.
- The final regulations should expressly prohibit the federal government from accessing, downloading, or mining the REAL ID databases, or linking other federal databases to the pointer record (should one be created).
- The final regulations should make it clear that no state is entitled to electronically access source documents or other personal information contained in the DMV databases of other states.

3. Limit the Data in the Machine-Readable Zone

- The final regulations should set the minimum amount of MRZ data elements at zero for states that wish to be highly protective of their residents' privacy, and set the maximum amount of MRZ data elements that contain personal information to: full legal name, date of birth, and driver's license/ID card number. State-of-issue may also be included, which DHS has not suggested.

4. Protect the Data in the Machine-Readable Zone

- The final regulations should mandate encryption of data contained in the MRZ or some other means to technologically protect data stored in the MRZ.
- If DHS refuses to mandate encryption, it should not prohibit encryption – states should be free to encrypt data in the 2D barcode if they so desire in order to ensure the privacy and security of their residents' personal information.
- The final regulations should prohibit non-law enforcement federal agencies from "skimming" data from the MRZ.

5. Protect Against Unauthorized State Employee Access to Federal Databases and Prevent the Document Verification Process from Being Used to Compile Additional Information at the Federal Level

- The final regulations should limit how states can access federal databases for the purpose of verifying source documents and should require states to ensure that only authorized DMV employees can access the federal databases and only for the purpose of issuing driver's licenses or ID cards.
- The final regulations should ensure that the federal government does not use the document verification process to compile additional data on REAL ID applicants.

6. Guard Against Mission Creep in the Federal Use of REAL ID

- CDT is pleased that DHS has chosen to limit the definition of "official purpose" to "accessing Federal facilities, boarding Federally regulated commercial aircraft, and entering nuclear power plants."
- CDT urges DHS to provide in the regulations that any future expansion of "official purpose" could occur only by legislation or by notice and comment rulemaking open to public comment consistent with the Administrative Procedure Act.

7. Ensure that the Driver's License/ID Card Number Does Not Become the New SSN

- The final regulations should limit the use of the REAL ID identifier and prohibit REAL ID numbers from having a standard format, being nationally unique, or remaining tied to individuals even when they move states.

8. Avoid the Security Flaws in the Western Hemisphere Travel Initiative (WHTI)

- "Vicinity read" RFID chips should not be included in WHTI-compliant driver's licenses and ID cards.
- CDT agrees that the creation of such a dual-use driver's license or ID card should always remain voluntary after individuals are fully informed of all the benefits, risks, monetary costs and other details of the program.

III. ANALYSIS OF PROPOSED REGULATIONS

A. DHS HAS PROPERLY LIMITED THE DEFINITION OF "OFFICIAL PURPOSE" [§37.3]

1. The Final Regulations Should Limit "Official Purposes" to Those Enumerated in the REAL ID Act

CDT is pleased that DHS has chosen to limit the definition of "official purpose" in §37.3 of the proposed regulations to "accessing Federal facilities, boarding Federally regulated commercial aircraft, and entering nuclear power plants." The REAL ID Act itself enumerates these purposes but also permits the Secretary to expand the definition.[8] However, the Department is seeking comment on "how DHS could expand this definition to other federal activities."[9]

CDT strongly urges the Secretary of Homeland Security not to expand beyond these three "official purposes" in the future. This limitation is important because significant privacy and security – including national security – risks are associated with using a single credential for a multitude of purposes.[10] However, if the Secretary wishes later to expand the definition of "official purpose" in the future, DHS must publish proper notice in the Federal Register and open up the proposal to public comment consistent with the Administrative Procedure Act.[11]

2. The Final Regulations Should Prohibit Federal Agencies From "Skimming" Data from the Machine-Readable Zone Even for "Official Purposes"

DHS should make clear in the final regulations that **the requirement that a REAL ID card be *presented* as proof of an individual's identity for the enumerated official federal purposes does not authorize federal agencies to "skim" data from the card's Machine-**

[8] REAL ID Act §201(3).

[9] NPRM, Preamble at 10823. *See also* NPRM, Preamble at 10842.

[10] *See., e.g.*, Bruce Schneier, "Real-ID: Costs and Benefits" (January 30, 2007) ("A single ubiquitous ID card will be trusted more and used in more applications. Therefore, someone who does manage to forge one – or get one issued in someone else's name – can commit much more fraud with it. A centralized ID system is a far greater security risk than a decentralized one with various organizations issuing ID cards according to their own rules for their own purposes.") <http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html>.

[11] 5 U.S.C. §553.

Readable Zone (MRZ). Nothing in the REAL ID Act authorizes federal agencies to read and collect information contained in the MRZ. The statute simply states that "a Federal agency may not accept, for any official purpose" a state driver's license or ID card that does not comply with the Act.[12] More importantly, the Conference Report states that the **MRZ must *only* be able to be read by law enforcement officials.**[13] That point was reiterated by Stewart Baker, DHS Assistant Secretary for Policy, before the DHS Data Privacy and Integrity Advisory Committee on March 21, 2007, who stated that the federal government has *no* intention of using the MRZ in any way. It is critical that DHS spell this out in the final regulations.

3. The Final Regulations Should Clearly State That Neither the REAL ID Act Nor the Regulations Change Current Admittance Practices of Federal Agencies

DHS states in the Preamble that **"These regulations are not intended to change current admittance practices at Federal facilities . . . if a Federal facility currently accepts identification other than a State-issued driver's license or identification card, the Act and these proposed regulations do not require that the agency refuse to accept such other forms of identification." CDT urges DHS to make this clear in the regulations themselves.** Thus, at present, individuals need not show ID before passing through airport security; they may instead submit to a more extensive physical search. The REAL ID Act would not change this option.[14]

B. STATE QUERYING OF FEDERAL DATABASES FOR SOURCE DOCUMENT VERIFICATION [§37.13]

Pursuant to §37.13 of the proposed regulations, states will be required to electronically "verify with the issuing agency the issuance, validity, and completeness of a document presented to demonstrate a person's eligibility for a REAL ID driver's license or identification card." It is critical both state and federal participation in this component of the program be clearly defined to prevent privacy abuses.

1. The Final Regulations Should Clarify Details of the Federated Querying Service and Prevent the Document Verification Process from Being Used to Compile Additional Personal Information at the Federal Level

The Preamble includes an extensive discussion of source document verification that is not reflected in the proposed regulations themselves. DHS asserts that "neither the REAL ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before," and "there is no information about a licensee that the Federal Government

[12] REAL ID Act §202(a)(1).

[13] Conference Report on H.R. 1268, House Report 109-72, at 179.

[14] *See* Ryan Singel, "DHS Honchos Get a Polite Earful on New ID Regulations," *Wired News* (May 1, 2007) ("The TSA provision that allows people to fly without identification so long as they agree to extra screening will also not be changed by the regulation, according to [Jonathan] Frankel.") <http://blog.wired.com/27bstroke6/2007/05/dhs_honchos_get.html>.

will store that it is not already required to store."[15] Yet the proposed regulations do not include this same assurance or offer any guidance to ensure compliance.

In the Preamble, DHS also asserts that it "will support the development of" a *federated querying service* "that will automatically distribute State DMV queries for REAL ID data verification to the appropriate reference databases and combine the multiple responses into a single reply," but that the Department "will not operate or control this service."[16] However, DHS again failed to include this assurance in the proposed regulations, contending that the statement in the Preamble should "resolve concerns about a centralized database operated by the Federal Government."[17]

Additionally, DHS asserts that state participation in the federated querying service will be voluntary, and that states may instead link directly to the federal databases or indirectly via a portal provided by the American Association of Motor Vehicle Administrators (AAMVA).[18] Yet none of these options are included in the proposed regulations themselves.

CDT urges DHS include in the final regulations the above points made in the Preamble and to do so clearly and comprehensively. The final regulations should ensure that the federal government does not use the document verification process to compile additional data on REAL ID applicants.

2. The Final Regulations Should Be Specific About the Content of Source Document Verification Business Rules/Procedures, and Protect Against Unauthorized State Employee Access to Federal Databases

While the proposed regulations themselves simply require states to adopt source document verification procedures, the Preamble talks extensively about helping states develop "business rules." DHS claims that it and the Department of Transportation "will assist the States in their efforts to develop improved business rules and data formats for communications with reference databases. These business rules will, in turn, become part of the security plans submitted to DHS."[19] Similarly, the Preamble claims that the proposed regulations "require individual states to document their business rules for reconciling data quality and formatting issues and urge[] States to develop best practices and common business rules by means of a collective governance structure."[20]

Yet again, neither §37.13 nor any other section of the proposed regulations includes such statements. **CDT urges DHS to include the above language in the final regulations. More**

[15] NPRM, Preamble at 10824.

[16] NPRM, Preamble at 10833. *See also id.* at 10825.

[17] NPRM, Preamble at 10825.

[18] NPRM, Preamble at 10833.

[19] NPRM, Preamble at 10833-34.

[20] NPRM, Preamble at 10825.

specifically, the final regulations should set out what the states' source document verification "procedures" or "business rules" should address, including who at the state level may access the federal reference databases, when and for what purposes. The final regulations should further make clear that only authorized DMV employees may access the federal databases solely for the purpose of issuing driver's licenses or ID cards.

3. DHS Should Address the Concern That Applicants for REAL ID Cards Will Be Compared Against Federal Terrorist Watchlists

After the May 1, 2007 REAL ID "town hall" meeting held in Sacramento, DHS's Jonathan Frankel told a *Wired News* reporter "that applicants for Real ID licenses won't be compared against the government's centralized terrorist watchlist unless states choose to do so, a policy choice made to prevent people from feeling a heavy hand from the government."[21] However, this important assurance is not reiterated in the NPRM.

CDT urges DHS to expressly prohibit states from comparing driver's license and ID card applicants against federal terrorist watchlists, which still have fundamental due process and redress shortfalls.[22] Notwithstanding these concerns, if DHS wishes to propose watchlist comparison as a vetting option under REAL ID, it must publish proper notice in the Federal Register and open up the proposal to public comment consistent with the Administrative Procedure Act.[23]

C. SYSTEM DESIGN TO ENSURE ONE (REAL ID) DRIVER'S LICENSE OR IDENTIFICATION CARD PER PERSON [§37.33]

1. The Final Regulations Should Omit §37.33(b) Because It Is Not a Separate Requirement From Ensuring One REAL ID Card Per Person

The Act generally requires that states "provide electronic access to all other States to information contained in the motor vehicle database of the state."[24] The REAL ID Act specifically prohibits participating states from issuing "a driver's license or identification card to a person holding [one] issued by another State without confirmation that the person is terminating or has terminated the driver's license [or identification card]."[25]

CDT does not believe that the "electronic access" provision of the Act, although broadly written, is a separate statutory mandate. Rather, it is intended to ensure that the each American

[21] Ryan Singel, "DHS Honchos Get a Polite Earful on New ID Regulations," *Wired News* (May 1, 2007) <http://blog.wired.com/27bstroke6/2007/05/dhs_honchos_get.html>.

[22] *See, e.g.*, Electronic Privacy Information Center, Spotlight on Surveillance, "Problem-Filled Traveler Redress Program Won't Fly" (Nov. 2006) <http://www.epic.org/privacy/surveillance/spotlight/1106/>.

[23] 5 U.S.C. §553.

[24] REAL ID Act §202(d)(12). *See also* REAL ID Act §202(d)(13).

[25] REAL ID Act §202(d)(6).

resident only holds one REAL ID card at a time – which is the central purpose of the law – and not to provide states unfettered access to motor vehicle databases for all purposes. This narrower interpretation is supported by a the Conference Report,[26] as well as DHS' own interpretation of the statute.[27] However, §37.33 of the proposed regulations restates both statutory provisions, making it unclear as to what precisely is being required or permitted.

CDT urges DHS to clearly adopt this narrower interpretation in the final regulations, to omit §37.33(b), and to *expand* §37.33(c), which requires states, before issuing REAL ID cards, to "check with all other States to determine if any State has already issued a REAL ID driver's license or identification card to the applicant."

2. The CDLIS or Other Central Database System Should Not Be Used to Ensure Only One REAL ID Card Per Person

There is a stark omission from §37.33 of the proposed regulations: there is no explanation of the architecture for the query system that will allow states to determine whether a driver's license or ID card applicant already holds a card from another jurisdiction. **In the final regulations, it is critical that DHS lay out in detail the architecture of this system, which must not include the use of a central database that stores highly sensitive personal information on virtually all Americans.** Such a system would create enormous privacy risks, in particular a risk of "mission creep," as well as security risks. Creating a central database that houses personal data on over 240 million individuals *will* create a nation-wide identification system that could be used by the government and others to track people for purposes other than administering driver's licenses, and will become a highly desirable "target rich" environment for hackers and identity thieves.[28]

DHS has repeatedly tried to allay fears that the REAL ID Act will create a national ID card or national database. For example, the Preamble states that "the recommended architecture for implementing these data exchanges does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the states. Moreover, no Federal agency will operate the data exchanges affecting non-commercial driver's licensing."[29] And Secretary Chertoff has been quoted as saying, "We at the Department of Homeland Security in the federal government will not build, will not own, and will not operate any central database

[26] Conference Report on H.R. 1268, House Report 109-72, at 183-84 (discussing how standardizing the contents of DMV databases and allowing for data exchange between states will help ensure "only one license for one driver").

[27] NPRM, Preamble at 10834 ("Data exchange among states is mandated by section 202(d)(12) of the Act, wherein each State must provide to each other State(s) electronic access to the DMV database of that State . . . to verify that the applicant does not hold a valid driver's license or identification card in another jurisdiction . . .").

[28] *See generally* Privacy Rights Clearinghouse, "Alert: REAL ID Act Will Increase Exposure to ID Theft" (Feb. 28, 2007) <http://www.privacyrights.org/ar/real_id_act.htm>.

[29] NPRM, Preamble at 10825.

containing personal information. The data will continue to be held at the state level as it has traditionally been since they began to issue driver's licenses."[30]

Simply because DHS or another federal agency does not own or operate the data exchange system does not mean that a central database will not be part of the system architecture. Nor does that assurance preclude the federal government from *having access* to individuals' data (*see supra* Part III.D.). By all accounts, DHS is strongly leaning toward expanding the Commercial Driver's License Information System (CDLIS),[31] which in fact relies on a central, unencrypted[32] database that houses a small but very significant amount of personal information (including name and Social Security Number)[33] and that links to other personal information contained in state databases, specifically people's driving histories.[34]

Once all non-commercial drivers and ID card holders (i.e., virtually all American citizens and residents) are added to such a "pointer system," a centralized database will exist that will pose enormous risks to individual privacy. Mission creep will be unavoidable. The temptation to access this database for a variety of purposes; to download or mine the database *in toto*; or to link

[30] Renee Boucher Ferguson, "DHS Issues Proposed Regulations for Real ID Act," *eWeek* (March 2, 2007) <http://www.eweek.com/article2/0,1895,2100036,00.asp>.

[31] The American Association of Motor Vehicle Administrators (AAMVA) manages a central database – the "Central Site" – that includes basic identification information for holders of commercial driver's licenses. A person's "pointer" record within the central database includes the individual's name, alias information, date of birth, Social Security Number (mandatory), and current State of Record (the issuing state). The State of Record, after issuing a person's first CDL, must report the person's basic identification information to CDLIS, which becomes the individual's "pointer" record. AAMVA's central database does not contain a person's commercial driving history; this information is housed in the database of the State of Record.

If person applies for a CDL is another state, the new state will check CDLIS (by inputting basic identification information), which will then "point" to the person's commercial driving history in the State of Record's database. If the person's commercial driving history is good, the new state will issue a new CDL, become the new State of Record, and transfer the person's commercial driving history over to its own database. A person cannot have more than one commercial driver's license (nor can a person have a non-commercial driver's license at the same time) and his commercial driving history follows him from jurisdiction to jurisdiction.

[32] It is CDT's understanding that the personal data stored at the CDLIS Central Site sits in the database in unencrypted form, and that communications are also unencrypted. AAMVA informed CDT that an effort has begun to encrypt both the static and dynamic CDLIS data. However, CDT uncovered a Federal Register notice related to CDLIS modernization that only refers to "provid[ing] encryption of the data traveling across the network as it is communicated from State to State in the normal operation of CDLIS," and not also the personal data stored in the central database. Federal Motor Carrier Safety Administration (FMCSA), Department of Transportation, *Commercial Driver's License Information System (CDLIS) Modernization Plan*, 71 Fed. Reg. 25885 (May 2, 2006) <http://www.fmcsa.dot.gov/rules-regulations/administration/rulemakings/notices/E6-6598-CDLIS-modernization-plan-5-2-06.htm?printer=true>.

[33] *See* AAMVA's webpage on CDLIS <http://www.aamva.org/TechServices/AppServ/CDLIS/>.

[34] NPRM, Preamble at 10826, 10834. Also, the Department's Selden Biggs testified before the DHS Data Privacy and Integrity Advisory Committee on March 21, 2007 that adding over 240 million Americans to CDLIS' approximately 13 million commercial drivers would be a "minor addition."

new state or federal databases to the pointer record will be irresistible, leading to just the type of nationally searchable database that the public fears. The fact that much of the data is accessed through a "pointer system " a does not lesson the risk to personal privacy. And of course the security risks of centralizing such highly valuable personal data would be equally large.

In the final regulations, **CDT urges DHS to prohibit the creation of a central identification database. Instead, CDT's primary recommendation (discussed below) is that a decentralized querying system be designed to enable states to determine whether a person already holds a driver's license or ID card issued by another jurisdiction, where that information comes directly from each state and not via a central repository.**

3. The Final Regulations Should Mandate the Creation of a Decentralized Querying System to Ensure One REAL ID Card Per Person

CDT believes that DHS should have presented and analyzed in detail different architecture models for the system states will use to check whether a REAL ID applicant already holds a REAL ID card issued by another jurisdiction. Not only did DHS not explain in the NPRM exactly how CDLIS works, it did not present the public with any other system options that might be more protective of privacy and security.[35]

a. A Distributed System Should Be Used for the State-to-State Check

To ensure that each person holds only one valid REAL ID card – driver's license or state ID – at a time, CDT recommends that DHS direct the states to develop a decentralized querying system where one DMV uses an applicant's basic identifying information to "ping" or send requests to the other 55 jurisdictions. The DMV would get back "yes" or "no" responses regarding whether there is an active license or ID card in that person's name elsewhere.

This would be done by designing a classic distributed system that uses a common protocol for formatting data and sending and receiving messages (i.e., requests and responses), such as an XML schema.[36] A distributed system does not have a central database that houses the wanted data. Instead, data is stored at the endpoints (in this case, the DMV databases). Distributed systems are in wide use today for a variety of commercial and government processes.

In a distributed system, communications regarding the data can happen in a number of different ways. One way is to have the communications completely decentralized. In this case,

[35] DHS seeks comments on "how the REAL ID Act can be leveraged to promote the concept of 'one driver, one record, one record of jurisdictions' and prevent the issuance of multiple driver's licenses." NPRM, Preamble at 10842. CDT does not see how DHS can force states that have made a wholesale decision not to participate in REAL ID to participate in this nationwide data exchange system. Thus the proposed system is to ensure one *REAL ID card* per person amongst those jurisdictions who choose to follow the REAL ID Act. However, states that issue REAL ID cards may also choose to issue non-REAL ID cards, but may choose to run non-REAL ID card applicants through the state-to-state querying system.

[36] *See* Joab Jackson, "An XML registry is key to sharing data," *Government Computer News* (Feb. 7, 2005) <http://www.gcn.com/print/24_3/35005-1.html>.

each jurisdiction would "ping" all the other jurisdictions with its queries, and each jurisdiction would collect its own responses. Here is a more detailed example of how a this might work under REAL ID:

> Suppose John Doe walks into a Virginia DMV to get a new driver's license. Before beginning the application process, the DMV official would type John's full name and date of birth into a secure Web form, and then click the 'Submit' button. The DMV computer would take the information from the web form and format it in a standardized way (perhaps using XML or another mark-up language). This information would then be sent in an encrypted email to each of the other 55 jurisdictions.
>
> In each jurisdiction, there would be a computer running a software program that receives these email requests. When a request is received, the software program would extract the name and date of birth from the message and look them up in that state's driver/ID database. The program would then send a response back to the Virginia DMV that made the original request. The response would say "Yes" if John Doe holds a valid license in that jurisdiction and "No" if he does not. The program would then delete the request and the personal information it contains.[37]
>
> The Virginia DMV computer would collect these 55 responses. If any of them contains a "Yes" response, the computer would give the DMV official a message saying that John Doe holds a valid license in another state. If all of the responses are "No," the computer would indicate that John Doe is allowed to apply for a license in Virginia.

This is a simplified example, but the whole process is actually one that would be simple to implement and automate using standardized protocols and formats that already exist today. In fact, it is CDT's understanding that AAMVA has been testing a decentralized querying model that allows states to check whether an applicant already holds a valid driver's license or ID card in another jurisdiction without having to query a central database as with CDLIS. CDT encourages DHS to further explore the distributed querying model.

A second way for communications to happen in a distributed system is to use a central processing server to direct the incoming queries to the various databases scattered throughout the network.[38] This type of system is currently being employed by NLETS.[39] NLETS is a message switching system for use by law enforcement. Law enforcement officers on the ground can send requests for criminal history information to NLETS, and NLETS will direct the queries to the

[37] This would be a key privacy provision under REAL ID. By way of comparison, NLETS being a message broker "logs each transaction by date, time, and originating agency and stores message content in the RAND archives database for audit and statistical reporting." NLETS Fact Sheet <http://www.nlets.org/resources/?cid=50>. CDT advocates for the *deletion* of personal information contained in the "message content" but does support the maintenance of a query log for auditing and security purposes.

[38] This is sometimes referred to as a "federated" model.

[39] Formerly called the National Law Enforcement Teletype System, its new full name is now the International Justice & Public Safety Information Sharing Network <http://www.nlets.org>.

appropriate jurisdictions. When NLETS receives responses, they are sent back to the originating law enforcement officer. Thus, the communications go through a centralized system, but the information is stored in decentralized databases. NLETS, which supports XML, thus stores no personal information on individuals.[40]

In addition, apparently this is the model that is being contemplated by DHS to verify applicant source data, such as Social Security Number and legal status, against federal databases. The Preamble states that DHS will support the creation of a federated querying service "that will automatically distribute State DMV queries for REAL ID data verification to the appropriate reference databases and combine the multiple responses into a single reply."[41] DHS has failed to explain why this or a truly decentralized querying system also cannot be used to ensure one REAL ID card per person.

b. Small States Should Receive Funding to Scale Up Their Systems to Accommodate the Anticipated Query Volume

CDT has heard concerns that a distributed system would be difficult to implement because small states would be overwhelmed by the volume of queries coming in each day from states that have large populations. **CDT recommends that DHS work with states to do detailed systems design and testing to determine if this would in fact be a meaningful problem and to what extent. If so, CDT believes the most logical solution is to provide smaller states with the appropriate funds to scale up their systems to handle the query volume likely be experienced under REAL ID.**

In addition, the move toward central issuance of driver's licenses and ID cards – where the cards are made at a central location and not in DMV branch offices – means that issuance of driver's licenses/ID cards can take several days. Because applicants no longer expect to receive their cards the same day, states could take advantage of this time delay and stagger their queries so as to not overload the databases of smaller states that are part of the distributed system.

4. A Second But Not Preferred Option is the Creation of a Pointer System Using a Centralized Hash Index

If DHS decides against the creation of a distributed querying system to ensure that each person holds only one REAL ID card at a time, a CDLIS-type "pointer system" can be used where the central database stores a "hash index" rather than personal information in clear text. The personal information of REAL ID card holders would be encoded using a one-way cryptographic "hash" function that produces a short representation of the information. It is easy to compute the hash value from the information, but it is difficult to reverse the process from the hash back to the information.[42] When an applicant comes into a particular jurisdiction to get a

[40] *See* NLETS Fact Sheet <http://www.nlets.org/resources/?cid=50>. *See also* "NLETS and XML" <http://www.nlets.org/projects/?cid=59>.

[41] NPRM, Preamble at 10833. *See also id.* at 10825.

[42] *See, e.g.*, National Institute of Standards and Technology (NIST), *Secure Hash Standard, Federal*

new REAL ID card, that jurisdiction would check if the hash of the applicant's personal information exists in the hash index. Such a match would indicate that the applicant will not be eligible for a new REAL ID card until he terminates the old one. The hash index would ensure that the centralized data is meaningless if accessed without authorization.

CDT has heard concerns that a querying system based on a centralized hash index would not allow for the searching of permutations of personal information, such as alternative spellings of names. While CDT recognizes this as a downside of using a hash index, CDT notes that the promise of REAL ID is to properly vet people and thereby add only accurate information (or information that has a high probability of being correct) to the state DMV databases. Thus it makes sense to run the multi-jurisdictional check only after the other verification steps have been completed for an applicant.

Finally, as with any unique number, the hash value could be used by government as a personal identifier similar to the Social Security Number if it can easily be tied back to the driver's license or ID card holder. **CDT recommends that if a hash index is used as the anchor for a national pointer system, policies must be in place prohibit the use of the hash value as a national identification number.**

5. A Centralized Database System Must Be Encrypted

If DHS chooses not to implement a decentralized querying system or one that uses a centralized hash index, but rather moves ahead with using CDLIS or a similar system with a central identification database, CDT urges DHS to mandate that the personal information in the database be encrypted, as well as communications to and from the Central Site.

6. The Final Regulations Should Set Up a Framework and Timeline for States to Clean Up Their Databases, and for Conducting Pilot Programs to Test the State-to-State Querying System Before It Is Rolled Out Nationally

The multi-jurisdictional check to determine whether an applicant holds a valid REAL ID card issued by another jurisdiction will only be successful if the databases of all participating states have accurate data. Thus states need to be given time to clean up their databases and properly vet their driver's license and ID card holders before the REAL ID program can be expected to also include an assurance that there is only one REAL ID card per person.

CDT urges DHS to set up a framework and timeline for states to first clean up their databases and then test the state-to-state querying system. Testing should occur via regional pilot programs so that technological and programmatic kinks can be worked out before the distributed querying system (or whatever system DHS chooses) is rolled out nationally.

Information Processing Standards Publication 180-2 (Aug. 1, 2002) <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.

D. PRIVACY AND SECURITY OF PERSONAL DATA STORED IN DATABASES AND SHARED ACROSS NETWORKS [§37.41]

1. The "Comprehensive Security Plan" Lacks Specific Privacy and Security Standards that States Must Meet to Achieve REAL ID Certification

CDT commends DHS for including in §37.41 of the proposed regulations a lengthy list of privacy and security issues that states must address in the Comprehensive Security Plan they must submit to the Department as part of their compliance procedures. CDT is particularly pleased that DHS has interpreted §202(d)(7)[43] of the REAL ID Act as also requiring states to ensure the security of the personal information stored in DMV databases.[44]

However, §37.41 falls short by failing to include any specific standards or minimum privacy and security criteria against which the state plans will be evaluated. For example, the Comprehensive Security Plan must include a "privacy policy regarding personal information collected and maintained by the DMV."[45] Yet there is absolutely no standards or criteria in the proposed regulations to guide state development or DHS approval of the privacy policies. In the absence of guidance, it is possible that there will be 56 different privacy and security policies with different levels of protection.

Other sections of the proposed regulations are rightly included, but could stand more detail :

- §37.41(b)(1)(iii): Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the physical locations and the personal information stored and maintained in DMV records and information systems.
- §37.41(b)(3)(iii): Access control, including . . . Controlled access systems.
- §37.41(b)(7): Internal audit controls.
- §37.41(b)(8): The State's standards and procedures for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction.

CDT recommends that DHS first conduct a survey of the various privacy and security policies for the protection of personal data adopted by various federal agencies and

[43] This section requires states to "ensure the physical security of locations where driver's licenses and identification cards are produced and the security of document materials and papers from which driver's licenses and identification cards are produced."

[44] NPRM, Preamble at 10841.

[45] §37.41(b)(5).

all state DMVs. Second, after compiling and distilling the data, DHS should consult with relevant federal and state officials, members of the privacy community, and security experts to determine what are the best privacy and security policies. Finally, DHS should then include specific minimum privacy and security standards in the final regulations that all jurisdictions must follow in order to receive REAL ID certification.

2. Privacy Guidance

Protecting privacy under REAL ID requires answers to the following questions: 1) What personal information may be collected and accessed 2) by whom, and 3) for what purposes? These questions need to be answered whether setting rules for direct access to personal information in state DMV databases, or indirect access through a national network.

a. The Driver's Privacy Protection Act is Ineffective to Protect Against Third Party Access to Personal Information Held Under REAL ID

As the PIA rightly explains, "DHS cannot rely on the [Driver's Privacy Protection Act] to protect the privacy of the personal information required under the REAL ID Act."[46] The DPPA basically "serves only as a prohibition on the sale of the personal information found in motor vehicle records for marketing purposes," since it permits disclosure of personal information "to any federal, state or local government agency to carry out that agency's legitimate functions."[47] Thus the DPPA is a floor and not a ceiling when it comes to the disclosure of individuals' personal information held by state DMVs.

Given that the REAL ID Act mandates the greater collection and storage of highly sensitive personal information (i.e., source documents) and directs a national system of information sharing between states and between states and the federal government, **CDT urges DHS to craft meaningful privacy regulations that will ensure a consistent approach to privacy and will diminish the risk of abuse.**

b. The Final Regulations Should Interpret the Privacy Act As Applying to the National Information Systems Developed to Implement REAL ID

Expansion of CDLIS to include all U.S. drivers and ID card holders brings with it an additional concern: the Privacy Act of 1974 – including its disclosure limitations and due process requirements – does not, under the prevailing agency interpretation, apply to the system.[48] Despite the fact that CDLIS was created pursuant to a congressional mandate, is funded by the Department of Transportation, and includes a national database, the Department of

[46] Department of Homeland Security Privacy Office, *Privacy Impact Assessment for the REAL ID Act*, at 12 (March 1, 2007) ("PIA") <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf>.

[47] PIA at 12. *See also* Driver's Privacy Protection Act of 1994 [H.R. 3355] Pub. L. 103-322, Title XXX, codified at 18 U.S.C. §2721 *et seq.*

[48] PIA at 11. *See also* the Department of Transportation Privacy Act Systems of Records list, which does not include CDLIS <http://www.dot.gov/privacy/privacyactnotices>.

Transportation has refused to interpret the Privacy Act as applying to CDLIS. Rather, it views AAMVA as the owner and operator of the system, rather than a government "contractor" which would be covered under the Privacy Act.[49]

Federal law does require the Secretary of Transportation to "develop a policy on making information available from [CDLIS]. The policy shall be consistent with existing Federal information laws, including regulations, and shall provide for review and correction of such information in a timely manner."[50] In the absence of Privacy Act protection, this mandate is virtually meaningless. Under DOT's new policy on the Availability of Information From CDLIS, federal agencies do have access to the system:

> [A]nother Federal agency may request access to information in CDLIS by written submission to FMCSA's[51] Chief Safety Officer. In the request, the applicant must state the legal basis and the need for access to CDLIS. A Federal agency will be required to execute a Memorandum of Understanding (MOU) with the Department of Transportation and/or FMCSA before access to CDLIS data will be provided.[52]

CDT recommends that the final regulations make clear that the querying systems – to either verify source documents against federal reference databases, or to ensure one REAL ID card per person – are subject to the federal Privacy Act of 1974.[53] The final regulations should also make clear that states still must meet certain minimum privacy standards for their end of the systems as laid out in §37.41, and should encourage states to include in their compliance plans additional privacy protections that are stricter than the minimum standards.

c. The Final Regulations Should Include and Expound on the Fair Information Principles

Both the Preamble and the Privacy Impact Assessment reference the Fair Information Principles:[54]

- Openness

[49] *See* Privacy Act of 1974, codified at 5 U.S.C. §552a(m).

[50] 49 U.S.C. §31106(e).

[51] The Federal Motor Carrier Safety Administration is part of the Department of Transportation.

[52] Department of Transportation, Federal Motor Carrier Safety Administration, *Policy on Availability of Information From the Commercial Driver's License Information System*, 70 Fed. Reg. 2454, 2455 (Jan. 13, 2005) <http://www.fmcsa.dot.gov/rules-regulations/administration/rulemakings/notices/05-669-CDLIS-Policy.htm>.

[53] Separate Privacy Impact Assessments for these two querying systems might be necessary as well. *See* E-Government Act of 2002 [H.R. 2458] Pub. L. 107-347, §208, 116 Stat. 2921 (Dec. 17, 2002).

[54] NPRM, Preamble at 10826. PIA at 13. *See also* OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html>.

- Individual participation (access, correction, and redress)
- Purpose specification
- Use and disclosure limitation
- Data minimization
- Data quality and integrity
- Security safeguards
- Accountability and auditing

CDT strongly supports these principles, which are related to the collection and use of personal information, and strongly urges DHS to include and expand upon these principles in the final regulations. While all of these FIPs are equally important, CDT believes that Purpose Specification, Use and Disclosure Limitation, Individual Participation, and of course Security Safeguards and Accountability (discussed below) will be important to stress in the oversight of the government's handling of personal information under the REAL ID Act.

Purpose Specification, and Use and Disclosure Limitation are two sides of the same coin. **CDT urges DHS to include in the final regulations a general rule limiting access to personal information, including source documents, to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. This includes accessing card holders' personal information directly from a state DMV database or via a national network.**[55]

This also means that DHS and other federal agencies cannot have wholesale, direct access to information contained in the REAL ID databases, or accessible via any networks that may be designed to implement the REAL ID Act. DHS asserts in the Preamble that "neither the REAL ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before," yet the Department has failed to include in the proposed regulations themselves any limitations on the federal government's access to REAL ID data.[56] As mentioned above with regard to the CDLIS central database, there will be a serious risk of "mission creep" as federal agencies are tempted – particularly without Privacy Act protection – to access, download, or mine the REAL ID databases *in toto*, or to link other federal databases to the pointer record (should one be created), thereby allowing much more personal data to be nationally searchable and accessible. **CDT urges DHS in the final regulations to expressly prohibit the federal government from tapping into the REAL ID system in these ways.**

On a related note, §37.59(a) of the proposed regulations requires that each state "provide any information requested by DHS." We assume that the intent of this provision was to permit DHS to conduct oversight of the program and determine compliance, but as written, this section

[55] The PIA for the National Driver Register (NDR) is very helpful in showing how access limitations can be laid out in detail for different users of a federal querying system. Department of Transportation, National Highway Traffic Safety Administration, *Privacy Impact Assessment for the National Driver Register (NDR)* (Nov. 17, 2003) <http://www.dot.gov/pia/nhtsa_ndr.htm#_Toc58811179>.

[56] NPRM, Preamble at 10824.

has the potential of creating a huge privacy loophole. **CDT recommends that the final rule state: "The State must provide any information requested by DHS *relevant to determining whether the State is in compliance with the REAL ID Act and these implementing regulations*."**

Individual participation (access, correction, and redress) is also a very important Fair Information Principle related to the management of personal information. The proposed regulations do have a provision that allows states to seek judicial review if DHS determines that a state is out of compliance with REAL ID.[57] **CDT urges DHS to include in the final regulations access, correction and redress procedures for individuals who are denied a REAL ID or are denied the right to use their REAL ID for an "official purpose" because of apparent non-compliance.**

d. Specific Use Limitations on Source Documents and Other Personal Information Held in DMV Databases

Neither the REAL ID Act itself nor the proposed regulations include any limitations on what information may go into a "motor vehicle database" (i.e., be part of a person's record) that may be shared and searchable by other states. The Act merely requires states to include at a minimum "all data fields printed on drivers' licenses and identification cards issued by the State," and "motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on a license."[58] The Act also requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information (e.g., birth certificate, passport, Social Security card, utility bill).[59]

As proposed above, CDT supports the creation of a decentralized querying system that enables one DMV to check all others to determine whether a driver's license or ID card applicant already holds a valid REAL ID card from another jurisdiction, where the querying system simply returns "yes" or "no" responses. At the March 21, 2007 DHS Data Privacy and Integrity Advisory Committee meeting, DHS official Selden Biggs endorsed this approach. He assured the Committee that the state-to-state data exchange system would only return "red light/green light" responses and that, importantly, **one state would not be able to freely access personal information contained in the DMV databases of other states, particularly source documents. CDT supports this limitation and urges DHS to make this clear in the final regulations.**

CDT is aware, however, that state DMVs may want to enable state-to-state exchange of certain other personal information – such as photos and driving histories – for specific DMV administrative or legal purposes. For example, the exchange of photos may help confirm an applicant's identity or uncover license or ID fraud.[60] The exchange of driving histories may

[57] NPRM, Proposed Regulations §37.59(e).

[58] §202(d)(13).

[59] §202(d)(1)-(2).

[60] *See* Conference Report on H.R. 1268, House Report 109-72, at 179.

reveal an exceedingly dangerous driver who is ineligible to obtain a REAL ID card in a new jurisdiction, which already occurs under CDLIS. **CDT urges DHS to include these specific use limitations, consistent with FIPs, in the final regulations.**

It is important to point out that should CDLIS or a similar model be used for REAL ID, it is not simply a " one license – one driver" system, but rather a "one person – one license (or ID card) – one *record*" system. In the REAL ID context, this is even more of a concern given that there are no statutory or regulatory limitations on what information may be in a person's "record," who can access the information, and for what purposes. Because this system would also include ID card holders, the "record" might not simply contain driving history.[61]

3. Security Guidance

The final regulations must include robust security standards for the national querying systems, as well as for the state DMV databases and their related IT systems. **The Federal Information Security Management Act of 2002 (FISMA) is an obvious place to start**.[62] However, more detailed criteria are needed to specifically apply to the REAL ID program. And states must know against which security standards their compliance plans will be evaluated.

It is worth noting that the Inspector General for the Department of Transportation recently found that DOT has consistently been failing to include CDLIS in its regular FISMA reviews.[63] DOT asserted that "CDLIS is only a grants program, meaning that the organization receiving the grant would be responsible for the system." But in the Inspector General's view, "CDLIS remains a DOT system," thus the Department "has a legal responsibility to protect the information" in the CDLIS system. Therefore, clearly identifying which agency has responsibility for a nation-wide information system created pursuant to congressional mandate is critical not only for the Privacy Act, but also for ensuring that minimum security standards are certified under FISMA.

As mentioned above, **CDT recommends that DHS determine the best security standards from the various security policies currently being implemented by federal**

[61] DHS is seeking comments "on whether and to what extent States can or should include in their security plans access to data for information sharing purposes as necessary in the event of a catastrophic event." NPRM, Preamble at 10841. From CDT's perspective, it seems reasonable that under the Individual Participation (Access, Correction and Redress) Fair Information Principles, an individual should have access to his source documents for whatever reason, including "when originals are destroyed." However, if DHS wants meaningful comments on this "catastrophic event" question, CDT urges DHS to issue a separate NPRM in which the Department better details how "the sharing of information collected and maintained by DMVs pursuant to the REAL ID Act" will help in recreating lost state data or in recovering efforts.

[62] *See* E-Government Act of 2002 [H.R. 2458] Pub. L. 107-347, Title III, 116 Stat. 2946 (Dec. 17, 2002). *See also* National Institute of Standards and Technology (NIST), FISMA Implementation Project <http://csrc.nist.gov/sec-cert/>.

[63] Office of Inspector General, Department of Transportation, *Information Security Program, Report No. FI–2007–002*, 8-9 (October 23, 2006) <http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/DOT_FISMA_Oct_20_FINAL_web-ready.pdf>.

agencies and state DMVs. As discussed above (and below in relation to the Machine-Readable Zone), encryption is a fundamental security tool. **Both personal information contained in databases and data traveling over networks should be encrypted.**[64]

Additionally, **the final regulations should set forth an accountability framework for those states that abuse personal data from other states.** As discussed above, the national querying system to ensure one REAL ID card per person might be expanded to allow data exchange – such as photos and driving histories – for specific DMV administrative purposes. The final regulations must address the potential problem of a state with a weaker security plan inappropriately accessing personal data held by another state. Rights of redress should flow to the victimized state as well as the victimized person.

Finally, §37.43 of the proposed regulations related to Physical Security of DMV Facilities simply provides that "State compliance with a performance-based standard approved by DHS will satisfy this requirement." **CDT takes no issue with a performance-based standard, but DHS must include those standards in the final regulations.**[65]

E. MACHINE-READABLE ZONE [§37.19]

The Machine-Readable Zone of the REAL ID card is addressed in §37.19 of the proposed regulations. States must use the PDF417 2D barcode and at a minimum include in it the following nine data elements, five of which are personal information:

1. *Full legal name and all name changes (i.e., full name history)*
2. *Date of birth*
3. *Gender*
4. *Address (presumably principal residence)*
5. *"Unique" identification number*[66]
6. Issue date
7. Expiration date
8. Revision date
9. Inventory control number

CDT is concerned that this section does not require technological security features, such as encryption, to protect the data on the card; it does not limit the amount and type of personal information that may be contained in the MRZ; and it does not limit who can "skim" data from the MRZ and for what purposes. The failure to explicitly address "skimming" opens the door to

[64] NLETS, for example, "encrypts data end-to-end." NLETS Fact Sheet <http://www.nlets.org/resources/?cid=50>.

[65] There might be a security risk if all the state security plans were housed in one place or in an insecure manner. Access to states' security plans would facilitate the cracking of the REAL ID security system, leaving personal information and physical supplies open for the taking. CDT suggests that DHS be mindful of how the REAL ID security (and privacy) plans are stored and accessed.

[66] *See supra* Part III.F.

using the REAL ID card as a key component of a vast and efficient surveillance system that enables widespread government tracking of the movements and activities of virtually all U.S. residents. Similarly, businesses and other non-governmental third parties could create profiles and fill databases with the activities and preferences of millions of U.S. residents.

1. CDT Supports the Choice of the 2D Barcode as the MRZ Technology But Emphasizes that the MRZ Was Not Meant to be a Security Feature

DHS has proposed that states use the PDF417 2D barcode standard for the MRZ. This was a logical choice since 46 jurisdictions already include a 2D barcode on their driver's licenses and ID cards and it is the existing standard for AAMVA.[67] CDT commends DHS for not requiring a contactless, radio frequency-based chip for the MRZ. CDT agrees with DHS that there is no need for driver's licenses and ID cards to be read at a distance.[68] More importantly, the use of RF technology in identification documents creates serious personal privacy and security risks.[69]

DHS did not explain why it discounted the contact chip. CDT would not oppose the use of a contact chip if proper privacy and security features were also included, but CDT supports DHS' choice of the 2D barcode given the costs and complexities associated with deploying computer chips. CDT takes no issue with the Department's conclusion that the 1D barcode lacks sufficient storage and that the optical stripe has durability issues over time. Thus, it seems that DHS has made a suitable choice in proposing the 2D barcode.

However, CDT wants to point out for the record that the 2D barcode has some shortfalls. DHS, states and other jurisdictions, law enforcement, and the public should be aware that the 2D barcode, like any technology, is not foolproof. The PDF417 2D barcode standard defines a way to encode data into a graphic image that can thereafter be optically scanned and decoded. This means that the data stored in a 2D barcode is static, so once the data has been encoded in the barcode image, it can never be changed.[70] Thus, if the barcode data needs to be encrypted (discussed below), it must be encrypted before it is encoded in the barcode image. If the encryption scheme used to protect the data is compromised, the data in the barcode is permanently exposed.[71]

[67] NPRM, Preamble at 10837.

[68] NPRM, Preamble at 10837.

[69] *See* Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security, *The Use of RFID for Human Identity Verification*, Report No. 2006-02 (December 6, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf>. *See also supra* Part III.G. regarding the Western Hemisphere Travel Initiative.

[70] *See* Wang, Y.P. U.S. Patent 5 243 655, 1993.

[71] With the 2D barcode, it is also not possible to upgrade the encryption scheme, employ dynamic forms of authentication such as challenge-response questions, store audit trails for accesses to the barcode data, or use other security features commonly used to protect data.

Additionally, because 2D barcodes are simple printed images, it is not difficult to create fraudulent barcodes. Anyone can print 2D barcodes using free software found on the Internet.[72] While indiscernibly integrating the fraudulent barcode into a REAL ID card should be more difficult under the new card security standards, it may nevertheless be possible. CDT emphasizes that the MRZ was not intended to be a security feature. Stewart Baker, DHS Assistant Secretary for Policy, made this point before the DHS Data Privacy and Integrity Advisory Committee on March 21, 2007. *The MRZ was not meant to authenticate the validity of identity information contained on the face of the card.* Rather, the MRZ was meant to be a tool of convenience for law enforcement officers, enabling them to more easily and accurately gather information on drivers during traffic stops. CDT urges law enforcement officers not to solely rely on the REAL ID barcode. Rather, they must ensure that the barcode data (i.e., full legal name, date of birth, driver's license/ID card number, and issuing state, as we propose below) matches the information on the front of the card. Otherwise, all of the benefits that come from technologies that secure the *front* of the card will be lost.

2. The Final Regulations Should Mandate Encryption of Data Contained in the MRZ

The REAL ID Conference Report explicitly contemplates some technological security feature, such as encryption, "to secure the privacy of the data contained on the machine readable strip."[73] Thus DHS does *not* have the option of leaving the data in the MRZ technologically open to reading and copying by anyone who has a 2D barcode scanner. The Conference Report also states that data in the MRZ should be "stored securely and only *able* to be read by law enforcement officials."[74] This means that not only are law enforcement officials the only ones who should be *authorized* to "skim" data from the MRZ, they are the only ones who should *technologically* be able to do so. (Though CDT finds it reasonable, as stated below, to allow DMVs to read the 2D barcodes as well.)

While CDT commends DHS for "leaning toward" encryption because it shows that the Department is aware of the privacy and security risks "associated with including personal information in an unencrypted" MRZ on the REAL ID card,[75] **CDT believes that DHS has a statutory directive to mandate encryption of the data contained in the 2D barcode (or employ some other means to technologically protect the MRZ).[76] However, if DHS refuses to mandate encryption, it should not *prohibit* encryption – states should be free to encrypt data in the 2D barcode if they so desire in order to ensure the privacy and security of their residents' personal information.**

[72] *See, e.g.,* CyanoSoft PDF417 Barcode Maker 2.1 <http://www.freedownloadscenter.com/Business/Printer_Tools/PDF417_Barcode_Maker.html>.

[73] Conference Report on H.R. 1268, House Report 109-72, at 179.

[74] Conference Report on H.R. 1268, House Report 109-72, at 179 (emphasis added).

[75] NPRM, Preamble at 10838.

[76] CDT reminds DHS that the ITAA (Information Technology Association of America) representative at the April 16, 2007 "negotiated rulemaking" meeting also advocated for encrypting the MRZ.

CDT recognizes that the unauthorized skimming of personal information off the MRZ already occurs in a number of states. Even though this phenomenon existed before REAL ID, CDT believes that it is the responsibility of DHS – given the federal mandate – to address this serious national problem in the next generation of driver's licenses and ID cards that will emerge as a result of the REAL ID Act.

Additionally, the fact that the face of the cards can be optically scanned and the data retrieved does not mean that encryption is pointless. Using a single MRZ technology with a standardized format – in this case, the PDF417 2D barcode – across the entire country greatly increases the incentive for bad actors to buy or develop the appropriate MRZ readers. Optical scanning can happen, but this will be more difficult if the face formats of state-issued REAL ID driver's licenses and ID cards remain different across jurisdictions.[77] And it is CDT's understanding that at present 2D barcode readers are cheaper and more ubiquitous than optical scanning technology. The PIA notes that 2D barcode scanners are available for purchase on the Internet at low cost.[78]

Understandably, DHS has concerns about the cost and practical feasibility of implementing a key management system.[79] DHS appears particularly concerned that encryption will actually *impede* certain law enforcement officials from accessing the information contained in the MRZ: "DHS believes that access to this information by law enforcement is essential to the requirements of the Act and invites comment on how to provide this access and the protection of the information at the same time."[80] CDT agrees that law enforcement officials are the intended beneficiaries of the MRZ, but concerns about cost and key infrastructure must not prevent an encryption scheme from moving forward, especially since security of personal data contained in the MRZ was an explicit expectation of Congress.[81] The PIA notes that encryption will be used in federal worker (HSPD-12) and transportation worker (TWIC) identification cards.[82] The 240 million Americans who will hold REAL ID cards deserve to benefit from the same prudent

[77] DHS should not mandate a standardized design or color for REAL ID licenses. NPRM, Preamble at 10842. This is not authorized under the statute. *See* REAL ID Act §202(b). Furthermore, this was strictly prohibited under the Intelligence Reform and Terrorism Act of 2004. *See* §7212(b)(3)(D). DHS should heed this policy choice, as states should be able to decide what design and other security features the face of the card will have to provide for ongoing improvements.

[78] PIA at 14. *See also* the Barcodes, Inc. website for a list of PDF417 barcode scanners for sale <http://www.barcodesinc.com/cats/barcode-scanners/pdf417.htm>.

[79] NPRM, Preamble at 10838 ("DHS leans toward an encryption requirement if the practical concerns identified above can be overcome in a cost-effective manner").

[80] NPRM, Preamble at 10838.

[81] Robert Burroughs, who has represented the Texas Department of Public Safety at several public meetings on REAL ID, has said more than once that 13 states have not given Texas their decryption keys for their commercial driver's licenses. But this seems to be an issue of state law and policy, rather than technological feasibility. States have a prerogative to protect the privacy and security of their drivers' information in this way.

[82] PIA at 17.

technological choice. Moreover, DHS should have conducted a comprehensive analysis of various encryption methodologies and their related estimated costs, and presented this information for public review and comment in the NPRM. DHS failed to do so and is now expecting the public to take over this responsibility.

CDT believes that the best option is *symmetric key cryptography*, where the encryption and decryption keys are the same.[83] There are several popular symmetric key cryptography algorithms in wide use today, including the Advanced Encryption Standard (AES), which was adopted as a federal standard by NIST in 2001.[84] As DHS states in the Preamble, there are two basic usage scenarios for symmetric key encryption of the 2D barcode: using a single key or a large number of keys.[85] In either case, a variety of hardware and software platforms exist on which decryption can occur in fractions of a second.[86]

a. Symmetric Key Encryption Using a Single Shared Key is Not Recommended

DHS rightly states in the Preamble that "there could be one single encryption key, which would avoid the complexities of needing a key infrastructure, but this greatly increases the risk that this single key could be compromised."[87] This would be highly insecure because as soon as the single encryption key is compromised, the personal data on every single driver's license and ID card across the country would be compromised as well.

The PIA notes that a new key could be used to encrypt barcode data on cards issued *after* the old key has been cracked.[88] While this would certainly be a necessary step, DHS should recognize that it leads to an endless game of cat-and-mouse, where hackers continually seek to compromise the current key and DMVs continually update the key in use. It also does nothing to protect the cards that were issued with the old key.

[83] In *public key cryptography*, the encryption and decryption keys are different, and every individual in the system has both a public and a private key. Data encrypted with an individual's public key can only be decrypted with that individual's private key. Due to the static nature of 2D barcodes, public key cryptography is nearly impossible for REAL ID driver's licenses and ID cards. The data in the barcode cannot be encrypted with the public key of the individual law enforcement officer who wishes to read it because the data must be set at the time the license is issued.

[84] National Institute of Standards and Technology (NIST), *Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197* (Nov. 26, 2001) <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[85] NPRM, Preamble at 10838. *See also* PIA at 16 n.50.

[86] *See, e.g.,* Joan Daemen and Vincent Rijmen, *AES Proposal: The Rijndael Block Cipher* (March 9, 1999) <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf>.

[87] NPRM, Preamble at 10838.

[88] PIA at 16.

b. Symmetric Key Encryption Using Many Shared Keys Is More Secure

Using a large number of cryptographic keys makes it more difficult to compromise the system because hackers will have many more targets of attack and each one will yield fewer cards whose data can be exposed. DHS has many options: each driver's license or ID card could have its own key; or there could be a key for each county, each zip code, or each state/jurisdiction; or small states like Rhode Island could have a single key while states with large populations like California could have multiple keys. Hackers would face anywhere from 56 to millions of keys, and each one cracked could only be used to decipher a limited number of REAL ID driver's licenses and ID cards. **CDT recommends choosing a middle-ground approach where there is not a single key for the entire country, but not millions of keys either.**

DHS notes in the Preamble that "this large number of cryptographic keys would need to be accessible to law enforcement personnel wherever they would be reading the driver's license."[89] **CDT believes that this will require law enforcement officers to be equipped with portable devices that either contain or can attach to 2D barcode scanners.** These devices should be capable of scanning the barcode, looking up the appropriate key, and decrypting the barcode information.[90]

The key look-up could be accomplished either locally or remotely. Consider the example with one key per ZIP code. In the *local* scenario, the key for each ZIP code is stored in a software database on the device itself. When a driver's license from ZIP code 12345 is scanned, the device would look up the cryptographic key for 12345 in the software database and decrypt the barcode information. The *remote* scenario requires that the device be able to connect to the Internet, because the key database would be stored remotely. The device would request the key for a particular ZIP code from the remote database, and that key would be returned to the device. In theory, the key database could be incorporated into another database to which law enforcement officers have access, such as the FBI's National Crime Information Center. **In either the local or the remote case, CDT stresses that the key database and communication of keys must be secured against unauthorized access.**

Each of these scenarios has drawbacks. In the local scenario, updates to the key database – when a new ZIP code is created or when a particular key is compromised, for example – will have to be pushed out to hundreds of thousands of devices. The remote scenario does not have this problem, since the database could be centrally managed and updated. It requires, however, that law enforcement officials have Internet connectivity wherever they intend to scan driver's licenses/ID cards. CDT understands that Internet access in patrol cars is not currently in wide use, and may not even be possible yet in some rural areas. However, should law enforcement's Internet connectivity become more widespread, the remote scenario would be a stronger option.

[89] NPRM, Preamble at 10838.

[90] CDT stresses that if Congress and DHS want REAL ID to implemented properly, significant infrastructure upgrades will be necessary.

c. Random Data Should Be Added to the Barcode

One way to make it more difficult for hackers to discover the a symmetric key is to add random data to the barcode information before it is encrypted. Secret keys can be discovered by using a "brute force attack" in which a large number of possible encryption keys are attempted in an effort to discover the correct one. If random data is mixed in with the real data elements, then it will be more difficult to determine when the correct key has been found in a brute force attack. This tactic merely strengthens the encryption system – it by no means makes the system foolproof. **CDT recommends that random data be inserted whether the barcodes are encrypted with a single key or with many keys, as discussed below.**

d. Encrypted Data As a National Identifier

Regardless of how the encryption system is implemented, there is one threat to privacy that is impossible to avoid if an encrypted MRZ is used. If every driver's license and ID card contains an encrypted data field, that data – in encrypted form – essentially becomes a national identifier. For example, retail chains could scan the MRZ and build up databases about individuals' behavior without needing to decrypt the data. Different retailers could combine their pools of data to create more detailed profiles about behavior across different contexts. **Having a single mandated national standard greatly increases the opportunity for an individual to be tracked, even with an encrypted MRZ.**

4. The Final Regulations Should Limit the Amount of Data Contained in the MRZ, Consistent With the Fair Information Principle of Data Minimization

DHS seeks comments "on what data elements should be included in the machine readable zone and the privacy considerations regarding the selection of such data elements and this technology."[91] In CDT's view, encryption or other technological means are clearly positive steps that can be taken to protect information on the MRZ. If DHS does not require encryption or other technological means of protecting MRZ data, this information can also be protected by policy and law. This should include narrowly limiting the information in the MRZ.

In the Preamble, DHS suggests that states should store "only the minimum data elements necessary for the purpose for which the REAL IDs will be used."[92] The PIA also discuss data minimization, a Fair Information Principle: "Good privacy policy supports limiting the data in the MRZ to the minimum personal data elements necessary for the intended purposes of providing access to law enforcement personnel."[93] Yet DHS makes no case regarding why it proposes including five elements of personal information in the MRZ: 1) full legal name and all name changes (i.e., full name history), 2) date of birth, 3) gender, 4) address (presumably principal residence), and 5) "unique" identification number.

[91] NPRM, Preamble at 10838.

[92] NPRM, Preamble at 10838 (emphasis added).

[93] PIA at 17. *See also* NPRM, Preamble at 10826.

In speaking with a representative of NLETS, CDT learned that to retrieve a person's driving or criminal history, a law enforcement officer simply needs that person's name and date of birth, *or* the driver's license/ID card number and the state that issued the card. In light of this fact and consistent with the Fair Information Principle of data minimization, **CDT recommends that DHS set the *minimum* amount of MRZ data elements at zero for states that wish to be highly protective of their residents' privacy, and set the *maximum* amount of MRZ data elements *that contain personal information* to: full legal name, date of birth, and driver's license/ID card number. State-of-issue may also be included, which DHS has not suggested.**[94] **Further, DHS should encourage states to include *either* full legal name and date of birth, or driver's license/ID card number and state-of-issue, but not all of these data elements.**[95] **The other suggested personal information – name history, gender and address – should not be added to the MRZ.**[96] As the PIA recognizes, having less information in the MRZ would make "skimming less attractive to third parties."[97]

5. The Final Regulations Should Prohibit "Skimming" By Federal and State Government Agencies, and Businesses and other Non-Governmental Third Parties

CDT is pleased that DHS recognizes "the privacy concerns raised by the potential for non-governmental third parties to collect and use the personal information on REAL ID driver's licenses and identification cards."[98] However, CDT is also concerned about unauthorized government "skimming" as well. As mentioned above, the REAL ID card is poised to be a key component of a vast and efficient surveillance system that enables widespread government tracking and profiling of the movements and activities of millions of Americans. As the PIA states, "The implementation of any digitized collection of information increases the efficiency by which that information can be accessed. Records, which were once accessible only in human-readable format, in digital form can be readily accessed and then used in ways *beyond the original purpose of the records*."[99]

It is critical that data in the MRZ be encrypted and be able to be decrypted only by law enforcement officials. It is also critical that DHS and all 56 jurisdictions put in place laws and policies that prohibit unauthorized "skimming" of data from the MRZ. These privacy measures

[94] *See* Proposed Regulations §37.19.

[95] CDT is not concerned about the other suggested MRZ data elements: issue date, expiration date, revision date, and inventory control number.

[96] DHS specifically "seeks comments on whether a demonstrable law enforcement need exists to include address in the MRZ." NPRM, Preamble at 10838.

[97] PIA at 17.

[98] NPRM, Preamble at 10826.

[99] PIA at 13 (emphasis added).

are especially important given that the Driver's Privacy Protection Act (DPPA) does not protect information contained on the card itself.[100]

CDT urges DHS to require states, as part of the certification process, to pass laws and/or regulations that limit the collection of personal data from the MRZ to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. DHS should also prohibit in the final regulations non-law enforcement federal agencies from "skimming" data from the MRZ of the REAL ID card. This would be consistent with the testimony of Stewart Baker, DHS Assistant Secretary for Policy, before the DHS Data Privacy and Integrity Advisory Committee on March 21, 2007 that the federal government has *no* intention of using the MRZ in any way.[101]

CDT disagrees with the Departments' assertion "that it would be *outside its authority* to address this issue within this rulemaking."[102] The Supreme Court has stated that "if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute. 'The power of an administrative agency to administer a congressionally created . . . program necessarily requires the formulation of policy and the making of rules to fill any gap left, implicitly or explicitly, by Congress.' *Morton v. Ruiz,* 415 U.S. 199, 231 (1974)."[103] CDT believes that prohibiting inappropriate "skimming" of data from the MRZ by both encryption and policy rules is a reasonable way to implement the REAL ID Act and ensure that it does not create more problems than it is trying to solve.

F. "UNIQUE" DRIVER'S LICENSE OR IDENTIFICATION NUMBER [§§37.17(d), 37.19(g)]

The REAL ID Act requires that the face of each card include "the person's driver's license or identification card number."[104] While the Preamble echoes the statutory language,[105] DHS refers to this number in the proposed regulations themselves as an individual's "unique"

[100] PIA at 14. *See also* 18 U.S.C. §2721; Driver's Privacy Protection Act of 1994 [H.R. 3355] Pub. L. 103-322, Title XXX.

[101] CDT is concerned with this DHS statement: "Authorized users of the information on the REAL ID driver's licenses and identification cards including, *but not limited to*, law enforcement should be able to access the necessary personal information stored on the driver's license or identification card in order to accomplish a legitimate law enforcement purpose." NPRM, Preamble at 10837 (emphasis added). As discussed above, Congress clearly meant to limit access to the MRZ data to law enforcement. CDT believes that the only other authorized individuals could be DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards.

[102] NPRM, Preamble at 10837 (emphasis added).

[103] *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 843 (1984) (footnote omitted).

[104] REAL ID Act §202(b)(4).

[105] NPRM, Preamble at 10835.

driver's license or ID card number: §37.17(d) of the proposed regulations requires a "unique driver's license or identification number," and §37.19(g) calls for the inclusion of an individual's "unique identification number" in the MRZ. CDT is concerned by what "unique" might mean since this is not spelled out in the proposed regulations.

1. The Final Regulations Should Prohibit REAL ID Numbers From Having a Standard Format, Being Nationally Unique, and Remaining Tied to Individuals Even When They Move States

CDT urges DHS to make clear in the final regulations that **driver's license and ID card numbers must only be "unique" within a state.** The final regulations should **prohibit identification numbers associated with REAL ID Act-compliant driver's licenses and ID cards from having a standard format, being unique nationally, and staying with a person if that person moves to a new state and is issued a new REAL ID card.**[106] It is critical that REAL ID card numbers not be standardized and unique nationally, and that they not remain tied to a person indefinitely like a Social Security Number. Otherwise, significant privacy and security risks would exist – most notably, the enhanced ability for both private and public sector tracking of individuals.

2. The Final Regulations Should Limit the Use of the REAL ID Identifier

The Privacy Impact Assessment rightly notes that a nationally unique REAL ID identifier will pose the same or greater privacy and security risks associated with the use of SSNs "if retailers, healthcare providers, financial institutions, insurers, and other private or government entities were to collect the credential and record the ID number whenever individuals engaged in a transaction."[107] Thus, **DHS should also require states, as part of the "privacy" certification process, to explain how they will limit the use of the REAL ID identifier, even if it is only unique within a state. DHS should also consider limiting federal use of the REAL ID identifier.** If DHS believes that this would be outside its authority under the Act, CDT encourages the Department to seek the necessary authority from Congress.

G. WESTERN HEMISPHERE TRAVEL INITIATIVE (WHTI)

DHS is seeking comments on whether state-issued "enhanced driver's licenses and identification cards could be acceptable at the land border to satisfy the WHTI requirements."[108] The statutory language referred to as the "Western Hemisphere Travel Initiative" requires DHS and the State Department to:

> develop and implement a plan as expeditiously as possible to require a *passport or other*

[106] The Privacy Impact Assessment assumes – without any statutory or regulatory basis – that "unlike a SSN, a person's driver's license number may change over time if the person moves from one state to another." PIA at 6.

[107] PIA at 6.

[108] NPRM, Preamble at 10842.

> *document*, or combination of documents, deemed by the Secretary of Homeland Security to be sufficient to *denote identity and citizenship*, for all travel into the United States by United States citizens and by categories of individuals for whom documentation requirements have previously been waived under section 212(d)(4)(B) of the Immigration and Nationality Act (8 U.S.C. 1182(d)(4)(B)).[109]

1. Will REAL ID Compliance Be a Prerequisite for WHTI Compliance?

CDT urges DHS to clarify whether the "enhanced" driver's licenses and ID cards will also have to be REAL ID-compliant. The Preamble states that "for purposes of satisfying WHTI requirements, the State would have to ensure that the State-issued REAL ID driver's license or identification card denoted citizenship for purposes of border crossing under WHTI."[110] Yet DHS recently entered into a Memorandum of Agreement with the State of Washington to launch a pilot program to develop "enhanced" Washington State driver's licenses and ID cards that are WHTI-compliant without an express requirement that the cards also comply with the REAL ID Act.[111] Moreover, Washington recently passed legislation refusing to comply with the REAL ID Act unless the federal government fully funds the state's implementation of the Act and the program includes all reasonable privacy and security measures.[112]

2. REAL ID-Compliant Cards Should Be Sufficient for Land Border Crossing

If a state must first comply with the REAL ID Act before WHTI maybe be considered, CDT urges DHS to clarify why the REAL ID cards themselves would not be sufficient documentation to re-enter the United States. The REAL ID issuance standards require *verified* proof of American citizenship or other lawful status within the U.S. There will be higher vetting standards overall and the cards themselves will be more resistant to tampering and counterfeiting. Thus, arguably, it may be presumed with a high degree of confidence that a holder of a REAL ID driver's license or ID card is a U.S. citizen or otherwise properly within the country, and nothing else would be needed to "enhance" the driver's licenses or ID cards.

[109] Department of Homeland Security Appropriations Act of 2007 [H.R. 5441] Pub. L. No. 109-295, § 546, 120 Stat. 1355 (Oct. 4, 2006), *amending* §7209(b)(1) of the Intelligence Reform & Terrorism Prevention Act of 2004 [S. 2845] Pub. L. 108-458, 118 Stat. 3823 (December 17, 2004) (emphasis added). 8 U.S.C. 1182(d)(4)(B) refers to "nationals of foreign contiguous territory or of adjacent islands and residents thereof having a common nationality with such nationals," meaning nonimmigrant aliens from Canada, Mexico and Bermuda.

[110] NPRM, Preamble at 10842.

[111] State of Washington Governor's Office, "Department of Homeland Security and the State of Washington Team Up To Advance Western Hemisphere Travel Initiative," News Release (March 23, 2007) <http://www.governor.wa.gov/news/news-view.asp?pressRelease=526&newsType=1>. Department of Homeland Security, "DHS and the State of Washington Team Up to Advance Western Hemisphere Travel Initiative," Press Release (March 23, 2007) <http://www.dhs.gov/xnews/releases/pr_1174904636223.shtm>.

[112] State of Washington Substitute Senate Bill 5087 (2007 Regular Session) <http://apps.leg.wa.gov/billinfo/summary.aspx?bill=5087&year=2007>.

However, it seems that DHS envisions requiring REAL ID card holders (as well as those with non-compliant driver's licenses and ID cards) to show separate proof of citizenship. Thus REAL ID card holders who are American citizens must show proof U.S. citizenship, and REAL ID card holders who are legally in the U.S. but are not American citizens must present a passport from their home country, as well as proof of their lawful status within the U.S., before re-entering the United States from Canada or Mexico.

3. "Vicinity Read" RFID Chips Should Not Be Included in WHTI-Compliant Driver's Licenses and ID Cards

Therefore, the question remains for American citizens – regardless of whether or not state-issued driver's licenses and ID cards are REAL ID-compliant – how can the cards be "enhanced" to be WHTI-compliant? In this rulemaking, DHS is seeking "comments on how States would or could incorporate a separate WHTI-compliant technology, such as an RFID-enabled vicinity read chip technology, in addition to the REAL ID PDF417 barcode requirement."[113]

DHS made this proposal in the NPRM in light of the PASS Card program that is already in development. The State Department and DHS have proposed creating a cheaper alternative to the passport for American citizens, called the PASS Card or passport card. The PASS Card is slated to have a "vicinity read" or long-range RFID chip in it that will include the person's unique identifying number, which will link to a back-end government database that houses personally identifiable information.[114] The MOA between DHS and the State of Washington is also limited to "enhancing" driver's licenses and ID cards of those state residents who are also American citizens, and such enhancement will also include "vicinity read" RFID technology.

CDT submitted comments on the choice of "vicinity read" RFID technology for the PASS Card[115] and recommended that this technology *not* be used in such an important identification and citizenship document because of the serious privacy and security risks associated with long-range RFID.[116] Thus **CDT strongly urges DHS not to require the inclusion of highly insecure "vicinity read" RFID technology in WHTI-compliant driver's licenses and ID cards.**

[113] NPRM, Preamble at 10842.

[114] Department of State, *Card Format Passport; Changes to Passport Fee Schedule*, 71 Fed. Reg. 60928 (to be codified at 22 C.F.R. pts. 22 & 51) (October 17, 2006).

[115] <http://www.cdt.org/security/20070108passcard.pdf>.

[116] *See also* Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security, *The Use of RFID for Human Identity Verification*, Report No. 2006-02 (December 6, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf>. *See also* Government Accountability Office, Testimony of Gregory C. Wilshusen, Director, Information Security Issues, Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security, *Information Security: Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology* (June 22, 2005) <http://www.gao.gov/new.items/d05849t.pdf>.

WHTI calls for the presentment of passports or passport-like documents at U.S. land borders, which was not previously required. CDT reminds DHS that WHTI does *not* call for any kind of technology, must less "vicinity read" RFID. As CDT discussed in its PASS Card comments, RFID chips that can be read from 20 feet away will not meaningfully increase processing efficiency when each person will need to be *individually* interviewed at the border. If border agents wish to have people's information pulled up and electronic checks conducted earlier, long-range RFID technology is wholly unnecessary. Rather, some sort of secure *contact* technology could be used and readers could be placed earlier in the line, such that people will have to present their PASS Cards for scanning 20 feet before they come into contact with the border agent.

In short, DHS has failed to explain why highly insecure "vicinity read" RFID technology is a good choice for an exceedingly important identity and citizenship document.

4. Citizenship Denotation Should Be Stored Electronically and Travel History Should Not Be Tied to the Driver's License/ID Card Number

DHS is also seeking comments on "whether citizenship could be denoted either on the face or machine-readable portion of the driver's license or identification card."[117] If denoting citizenship on the face of the card becomes the preferred WHTI-compliant route, CDT is concerned that law enforcement officials and others looking at the driver's license or ID card will draw negative inferences if they do not see "U.S. citizen" denoted on someone's card. **Thus CDT supports denoting citizenship electronically on the card. But it is extremely important that this be done *right*.**

CDT recommends that a WHTI-compliant driver's license or ID card contain two separate Machine-Readable Zones, one only for DMV and law enforcement use (in the case of a REAL ID card, this will be the 2D bar code) and one that is used solely for re-entering the United States at the land borders. Thus, as discussed above, the 2D barcode should be encrypted such that only DMV officials or law enforcement officials can access personal information for legitimate administrative or law enforcement purposes, respectively. Similarly, the WHTI MRZ must be exceedingly secure so that only border agents can read or collect information contained on the MRZ. It would not be unreasonable to have the WHTI MRZ technology be the same as that used in the U.S. electronic passports.

It is essential that both MRZs and their respective back-end databases be completely "fire-walled" from each other. The WHTI MRZ should simply include the denotation of American citizenship, and if necessary a separate WHTI or "passport" number issued by the State Department that links only to the State Department database. For privacy and security reasons, it is critical that the WHTI number not be included in the 2D barcode or in the DMV database. It is also critical that an individual's state-issued driver's license or ID card number not be tied to the person's international travel history. Again, **for WHTI-compliant driver's licenses and ID cards to be feasible, the two identifiers, Machine-Readable Zones and back-**

[117] NPRM, Preamble at 10842.

end databases must be completely separate from one another. And both MRZs must be highly secure such that only authorized government personnel can access the information contained therein.

5. Creation of a WHTI-Complaint Driver's License or ID Card Should Be Voluntary and the State Department Should Be Responsible for Vetting Individuals

Finally, DHS is seeking comments "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 includes citizenship information for WHTI compliance."[118] Most importantly, **CDT agrees that the creation of such a dual-use driver's license or ID card should always remain voluntary after individuals are fully informed of all the benefits, risks, monetary costs and other details of the program, consistent with the Fair Information Principles.**[119]

Secondly, if an American citizen wishes to have his state-issued driver's license or ID card accepted for land border re-entry into the U.S. from Canada or Mexico, **CDT recommends that the person be vetted by the State Department as if he were applying for a full-blown passport.** The State Department will verify that he is in fact an American citizen, assign him a WHTI or "passport" number, and inform his state DMV that he has been approved to received a WHTI-compliant driver's license/ID card. **The state DMV can create the license/ID card as it normally would, and then send it to the State Department to have the WHTI MRZ with relevant information added.**

IV. CONCLUSION

CDT urges DHS to include in the final regulations robust privacy and security protections for personal information held in government databases pursuant to the REAL ID Act, consistent with CDT's recommendations above. Effective driver's license and identification card reform cannot happen unless privacy and security are incorporated from the beginning and throughout all components of the program.

Additionally because there are key aspects of the Department's REAL ID implementation plan that were not elaborated upon in the NPRM, CDT believes that one or more additional notices should be published in the Federal Register so that DHS can present more detailed proposals for certain program components – such as the national querying systems, or the specific privacy and security standards against which state compliance plans will be evaluated – and thereby receive more meaningful public comments.

[118] NPRM, Preamble at 10842.

[119] *See* NPRM, Preamble at 10826. *See also* OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html>.

CDT looks forward to continuing to work with the Department of Homeland Security on this important national issue.

Sincerely,

/s/

Sophia Cope
Staff Attorney/Ron Plesser Fellow
Center for Democracy & Technology