Testimony of SOPHIA COPE
Staff Attorney/Ron Plesser Fellow, Center for Democracy & Technology

Before the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

On *"The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative"*

Tuesday, April 29, 2008

Chairman Akaka, Ranking Member Voinovich, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology,[1] I am honored to have been asked to testify before the Subcommittee on the personal privacy and security risks of "vicinity" radio-frequency identification (RFID) technology in travel documents issued in compliance with the Western Hemisphere Travel Initiative (WHTI), specifically the State Department's passport card and the state-issued "enhanced driver's license" (EDL).

Because this hearing also focuses on REAL ID, I attach as an Appendix CDT's REAL ID memo from February 1, 2008, analyzing the personal privacy and security risks of the REAL ID Act and the Department of Homeland Security's (DHS) final regulations, and proposing legislative options for Congress.[2] However, my written testimony below focuses on WHTI, as will my oral testimony.

INTRODUCTION

From warrantless electronic spying, to expanded DHS funding of closed circuit television (CCTV) video camera surveillance systems without privacy standards, to numerous data breaches at federal agencies, the federal government does not have a good track record of protecting personal privacy. The use of insecure vicinity RFID technology in border crossing identification documents is no exception: With no proven benefit to the nation's security, the Executive Branch has chosen a technology that jeopardizes privacy.

---

[1] The Center for Democracy & Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values in the digital age. Among our priorities is to ensure that government identification programs and the technologies they employ do not threaten personal privacy, security and civil liberties.

[2] CDT's REAL ID memo from February 1, 2008, is also available at: http://www.cdt.org/security/identity/20080201_REAL_ID_hillbrief.pdf.

Though the passport card is issued by the State Department and EDLs are issued by states,[3] DHS has played a key role in both programs, pushing for the use of insecure vicinity RFID technology in the border crossing context. However, the use of vicinity RFID technology in human identification documents:

- Poses clear and serious risks to personal privacy and security (**Section I**);
- Disregards concerns expressed by both Congress and the public (**Section II**); and
- Affords no clear operational benefits in the border crossing context (**Section III**).

CDT concludes that the use of vicinity RFID technology in human identification documents, such as the passport card and EDL, is inappropriate at this time due to the lack of meaningful security measures. The good news is that it is not too late to reverse course – no passport cards have been issued yet with the insecure technology and only one state has moved forward with using the insecure technology in driver's licenses. CDT urges this Subcommittee to exercise its oversight authority to ensure that our nation is secure, our travel is not impeded, and our privacy is protected. Specifically, we urge Congress to direct DHS and the State Department to revise its plans and use machine-readable technologies in the passport card and EDL that provide privacy protections commensurate with those in the electronic passport.

CDT is also concerned with the potential uses of the REAL ID card, the passport card and the EDL to facilitate tracking of the movements and activities of Americans in contexts having nothing to do with highway safety, border control or airline passenger screening. The less secure the ID number and other information on these documents is, the more likely that they will be used by government and business to compile databases that can be used to track and profile citizens. To avoid this problem, it is necessary to encrypt the information on the card and limit its use by the public and private sector.

I. VICINITY RFID TECHNOLOGY IN ID DOCUMENTS POSES SERIOUS RISKS TO PERSONAL PRIVACY AND SECURITY

What is "Vicinity" RFID Technology?

RFID chips containing a serial number and relevant information about the tagged item communicate wirelessly with a reader, which is itself connected to a back-end computer and database system. "Vicinity" refers to those RFID chips that can be read at some distance (as opposed to "proximity" RFID, which refers to chips that can be read only within millimeters or inches). Vicinity RFID chips are generally readable from 20 to 30 feet.[4] However, it was recently

[3] Washington, Vermont, New York, and Arizona have signed Memoranda of Agreements (MOAs) with DHS. Washington began issuing EDLs in January 2008, and Vermont will issue them later this year.

[4] Department of Homeland Security Privacy Office, "Privacy Impact Assessment for the Use of Radio Frequency Identification (RFID) Technology for Border Crossings" at 3 (Jan. 22, 2008) ("DHS RFID PIA"), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf.

reported that a company has developed a new reader system to read passive (that is, non-battery powered) "Gen 2"[5] chips from 600 or more feet away and pinpoint their location in 3-D space![6]

Three Technical Features of Vicinity RFID Technology Implicate Privacy

Many of the privacy and security problems associated with the passport card and EDL can be traced to the government's inexplicable decision to adopt so-called "Gen 2" vicinity RFID technology. The Gen 2 vicinity RFID chip is unsuited for use in human identification documents such as the passport card and EDL because:

1. **The information on the chip can be picked up directly ("skimmed"), or intercepted[7] during a legitimate transaction, by an unauthorized or "rogue" reader because the information is transmitted wirelessly in the clear.**
2. ***Any* compatible, widely available, reader – not just those used by Customs and Border Protection (CBP) at the border – can copy the information on the chip.** As the DHS Privacy Office has acknowledged, "any Gen 2 reader can read any Gen 2 card."[8]
3. **Vicinity RFID chips, due to the nature of radio waves, can be surreptitiously read from afar without line-of-sight and without the cardholder's knowledge or consent.**

The Gen 2 chip was designed to track *things*, not identify people. It was designed to manage the movement of products through the supply chain, taking the place of the traditional barcode. The main design considerations for the Gen 2 chip were speed and interoperability: The Gen 2 chip was designed to be quickly and easily scanned by standardized readers, unencumbered by security features such as authentication and encryption, as products move through the supply chain.[9]

---

[5] The standards body EPCglobal has developed the protocol for the Class 1, Generation 2 (**"Gen 2"**) Ultra-High Frequency (UHF) RFID chip, which is used in the passport card and EDL, http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_0_9-standard-20050126.pdf.

[6] Mark Roberti, "Mojix Takes Passive UHF RFID to a New Level," *RFID Journal* (April 14, 2008), http://www.rfidjournal.com/article/articleview/4019/1/1/.

[7] Interception is also called "eavesdropping." Data Privacy & 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, Section VI.C. (December 6, 2006) ("DHS Privacy Committee RFID Report"), http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

[8] DHS RFID PIA, *supra* note 4, Section 9.2.

[9] *See, e.g.*, David L. Brock, *White Paper: The Electronic Product Code (EPC), A Naming Scheme for Physical Objects*, Massachusetts Institute of Technology Auto-ID Center, Section 4.14 (January 1, 2001) ("[W]e propose to leave Electronic Product Code simply as a method for naming and identifying objects," and thus "propose to decouple the EPC definition from any security and cryptographic technique."), http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-002.PDF.

What Are the Privacy Risks of Vicinity RFID Technology and the Passport Card/EDL Programs?

- **Passport card and EDL holders' movements and activities may be tracked with the vicinity RFID chip.**[10] DHS' and the State Department's number one response to concerns raised about the privacy risks of using vicinity RFID technology in the passport card and EDL is that the chips will not contain any personal information, just a **unique ID number** that corresponds to the citizen's record stored in a back-end database.[11] This overlooks the fact that governmental and commercial entities can collect the identifying information about the individual by other means – by visually inspecting the card, by scanning the non-RFID machine-readable zone on a driver's license, or by collecting the identifying information from a customer loyalty card or credit card used in a transaction when the passport card or EDL is also used. This identifying information can then be associated with the unique ID number skimmed or intercepted from the vicinity RFID chip. In this way government agencies and businesses can compile unauthorized databases associating RFID ID numbers with names and other personally identifying information. Once a person's identity is associated with the unique ID number, that person can thereafter be identified or tracked without his or her knowledge or consent by a network of Gen 2 compatible readers.[12] **The risk of creating unauthorized databases correlating ID numbers and other personal information would be reduced *but not eliminated* if the government were to shift from vicinity RFID to a machine-readable technology that requires the card to make physical contact with the reader (i.e., non-wireless), or at the very least proximity RFID.** To effectively protect individuals, the government should also **encrypt the ID number**, so it cannot be skimmed by governmental and commercial entities and used as the basis for compiling new databases of movements and activities unrelated to highway safety or border control.

- **A person traveling abroad might be revealed as an American citizen and thereby be vulnerable to security risks.** In addition to the unique ID number, the vicinity RFID chip (Gen 2) also includes additional numbers that reveal information about the cardholder: namely, the issuing authority of the card, whether that be DHS, the State Department, or an American state (among others).[13] Thus if an ill-intentioned individual with a rogue Gen 2

---

[10] DHS RFID PIA, *supra* note 4, Section 1.5, at 8.

[11] *See, e.g.*, Department of Homeland Security, "Fact Sheet: Enhanced Driver's Licenses (EDL)," ("The first layer [of privacy mitigation] will be that no personally identifiable information will be stored on the card's RFID tag or be transmitted by the card. The card will use a unique identification number which will link to information contained in a secure database. This number will not contain or be derived from any personal information.") ("DHS EDL Fact Sheet"), http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm.

[12] *See, e.g.*, Todd Lewan (Associated Press) "Chips: High-tech aids or tools for Big Brother?," MSNBC (July 23, 2007), http://www.msnbc.msn.com/id/19904543/.

[13] DHS RFID PIA, *supra* note 4, Section 1.1 ("when the Gen 2 tag data is sent from the RFID card to the RFID reader, CBP will be able to identify the type of card in terms of providing a numeric identifier that can be associated by the back-end computer system with the particular issuer of the border crossing card"); Section 1.2 ("The border crossing travel document assigned to the traveler following enrollment contains an RFID chip with a unique ID number preceded by a header that identifies the issuing authority of the card. During border crossings, CBP collects the RFID number and header from the RFID enabled cross border travel document

reader picks up the presence of a vicinity RFID chip, and that person has figured out what the header number signifies (i.e., an issuing entity originating in the U.S.), the security of the American citizen may be put at risk.

- **Even if the vicinity RFID chip were protected from skimming or eavesdropping by unauthorized users, *rules should be adopted* to address the fact that *authorized* users will be able to use the card to build new databases of citizens' activities. For example, without further safeguards, state authorities will be able to compile logs of border crossing history as *CBP pings state databases* whenever an EDL is used to cross the border.**[14] To avoid this problem and ensure that personal data is protected to the maximum extent possible, but also to provide one convenient document that can be used for two purposes, *the EDL should have two machine-readable zones:* one only for legitimate motor vehicle and law enforcement use (such as a magnetic stripe or a bar code), populated by the state only with information related to this purpose (e.g., name and driver's license number); and one only for re-entering the U.S. at the land borders, populated by the State Department only with information enabling the confirmation of the cardholder's U.S. citizenship (e.g., a unique ID number that *links to a State Department database*). Both back-end systems should be "fire-walled" from each other, avoiding the need for CBP to ping state databases and preventing the state from knowing when a licensee traveled to Canada or Mexico. CDT suggested this approach to DHS in our comments on the proposed REAL ID regulations,[15] but the Department is nevertheless moving forward with its original cross-access model.[16]

- **Border crossing history and personal information associated with the passport card or EDL may be vulnerable to unauthorized access.** DHS acknowledges that "the RFID number could be used to access the back end system and reveal the PII contained in those systems"[17] or "transaction data."[18] DHS claims that even though the unique ID number may be easily obtained from a vicinity RFID chip, access to personal information associated with that number is limited by use rules and technical security features. However, recent privacy breaches at the State Department show it is possible for unscrupulous government

---

assigned to the individual during the aforementioned enrollment process."); Section 1.5 ("The new RFID tags to be used in the CBP border crossing documents . . . do contain header information which could reveal some overall category information, that is the type of RFID enabled card being carried.").

[14] DHS RFID PIA, *supra* note 4, Section 1.2 ("DHS will receive information associated with the RFID number which will reference biographical and biometric (photo) information maintained in the issuing entities back-end database. Issuing entities could include state Department of Motor Vehicles (DMV) for enhanced driver's licenses"). *See also* Washington State Department of Licensing's flier on EDL "Security and Privacy Protection" ("The unique reference number will be matched to Department of Licensing (DOL) records to verify the information contained on the front of the EDL/ID card."), http://www.dol.wa.gov/about/news/priorities/security.pdf.

[15] http://www.cdt.org/security/20070508realid-comments.pdf (p. 33).

[16] Department of Homeland Security, *Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (Final Rule), 73 Fed. Reg. 5272, 5313 (Jan. 29, 2008) ("REAL ID Final Rule").

[17] DHS RFID PIA, *supra* note 4, Section 1.5, at 8.

[18] DHS RFID PIA, *supra* note 4, Section 1.5, at 7.

employees or contractors to access citizens' sensitive data held in government databases.[19] **Moreover, the DHS Inspector General concluded that Customs and Border Protection (CBP), the agency which reads border crossing documents, "has not implemented effective security controls over all components of its RFID systems" used in the Trusted Traveler programs.[20]** The Inspector General "identified several weaknesses in user administration, access controls, and auditing," and went on to conclude that such "weaknesses may be exploited by a user to gain unauthorized and undetected access to sensitive data. Lacking procedures to ensure that all vulnerabilities and weaknesses are identified and reviewed, management cannot ensure that the data in its critical systems is secure."[21]

Privacy Risk Mitigation Strategies Are Insufficient

To mitigate the privacy risks associated with an insecurely-transmitted unique ID number, DHS explains that cardholders will be provided with a **"protective sleeve"** that blocks radio communications, in which the vicinity RFID-enabled card should be housed when not being used at the border. DHS also explains that all holders of vicinity RFID-enabled travel documents will be **educated** on how to properly use, carry and protect the cards so as to minimize risks to personal privacy.[22]

However, these mitigation measures improperly place the burden of privacy protection on the citizen. Moreover, they offer no protection in light of the fact that the EDL and the passport card will be used in many circumstances where driver's licenses or ID cards are now required, including in many commercial contexts, where individuals will be taking their cards out of the protective sleeve, thereby exposing their data to all the risks we have described above. Circumstances include buying alcohol, paying by check, entering many governmental and commercial office buildings, registering at a hotel, renting an automobile, and many others.

Finally, DHS and the State Department (and even EDL-issuing states) often counter privacy criticisms by emphasizing that the passport card and EDL programs are **voluntary**. While vicinity RFID-enabled travel documents are currently voluntary, there is a reasonable concern that people will no longer have a choice as RFID becomes the standard technology in identification documents.

---

[19] Glenn Kessler, "Rice Apologizes For Breach of Passport Data," *Washington Post* (March 22, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032100377.html.

[20] The Trusted Traveler programs, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/, use first generation ("Gen 1") vicinity RFID chips. DHS RFID PIA, *supra* note 4, at 4 ("Currently, CBP's trusted traveler programs use Gen 1 tags.").

[21] Department of Homeland Security, Office of Inspector General, *CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security (Redacted)*, OIG-06-36, at 6-7 (May 2006) ("DHS IG Trusted Traveler Report"), http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr-06-36_May06.pdf.

[22] DHS RFID PIA, *supra* note 4, Section 1.5. *See also* DHS EDL Fact Sheet, *supra* note 11.

II. DHS AND THE STATE DEPARTMENT ARE MOVING FORWARD WITH THE PASSPORT CARD AND EDL PROGRAMS DESPITE PUBLIC DISAPPROVAL AND IN CONTRAVENTION OF LEGISLATIVE MANDATES AND INTERNAL WARNINGS

- **The passport card and EDL programs' use of vicinity RFID technology is not statutorily mandated.** DHS and the State Department are moving full steam ahead with the development of these vicinity RFID-enabled travel cards as if the technology choice were mandated by Congress. But this is not the case. Congress simply sought to expedite the travel of pre-screened frequent travelers at the land borders. It never mandated the use of vicinity RFID technology in this context.[23] **Other technologies can achieve the same goal (see Section III below).**

- **DHS and the State Department failed to obtain sufficient NIST certification that the passport card (and thus EDL) will protect privacy.** It was not until Congress became aware that DHS and the State Department were in the midst of developing the passport card using insecure vicinity RFID technology that Congress specifically legislated on this issue.[24] While Congress mandated NIST certification on October 4, 2006, the State Department announced its proposed choice of vicinity RFID technology for the passport card in a notice published in the Federal Register 13 days later (October 17, 2006), *which made no mention whatsoever of the recently required NIST certification.* What the

---

[23] Section 7209(b)(1) of the Intelligence Reform & Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458 (Dec. 17, 2004), simply required DHS and the State Department to "develop and implement a plan as expeditiously as possible to require a passport or other 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 . . . This plan . . . shall seek to **expedite the travel of frequent travelers**, including those who reside in border communities, and in doing so, shall make readily available a registered traveler program (as described in section 7208(k))." Similarly, Section 7208(k) does not mention vicinity RFID technology, but instead simply states that "Expediting the travel of previously screened and known travelers across the borders of the United States should be a high priority," and that "The process of expediting known travelers across the borders of the United States can permit inspectors to better focus on identifying terrorists attempting to enter the United States." Sections 7208(k)(1)(A) and (B).

[24] Section 546 of the DHS Appropriations Act for FY2007, Public Law 109-295 (Oct. 4, 2006), amended Section 7209(b)(1) of the IRTPA to require DHS and the State Department to receive certification from the National Institute of Standards and Technology (NIST) that the Departments, for the passport card, "selected a card architecture that meets or exceeds International Organization for Standardization (ISO) security standards and **meets or exceeds best available practices for protection of personal identification documents**: Provided, That the National Institute of Standards and Technology shall also assist the Departments of Homeland Security and State to **incorporate into the architecture of the card the best available practices to prevent the unauthorized use of information on the card**: Provided further, That to facilitate efficient cross-border travel, the Departments of Homeland Security and State shall, to the maximum extent possible, develop an architecture that is **compatible with information technology systems and infrastructure used by United States Customs and Border Protection.**" As discussed below in Section III, the question of **compatibility** is an interesting one: The new electronic passport includes a proximity RFID chip and other security features, which together require a different reader system, as does the "Gen 1" vicinity RFID technology CBP uses for its Trusted Traveler programs.

government calls NIST "certification" did not come until May 2007,[25] but NIST simply accepted at face value the vicinity RFID technology choice. This can hardly be said to constitute an objective analysis by NIST of whether the passport card "meets or exceeds best available practices for protection of personal identification documents" or is designed "to prevent the unauthorized use of information on the card" as required by Congress. **Moreover, two sets of "best practices" cited by NIST do not support the use of vicinity RFID technology in the passport card and EDL but actually undercut it:** The DHS Data Privacy & Integrity Advisory Committee's report on "The Use of RFID for Human Identification" cautions against the use of RFID for identifying people,[26] while CDT's "Privacy Best Practices for Deployment of RFID Technology" only relate to the use of RFID in the *commercial* context and expressly do *not* apply to the use of RFID for personal identification.[27]

- In his "certification" letter dated May 1, 2007, NIST Director William Jeffrey revealed that **DHS and the State Department were already committed to vicinity RFID for the passport card and so NIST did not challenge the wisdom of choosing this insecure technology**.[28]

- An additional piece of evidence that the State Department was planning on ignoring public comments is that it **issued a Request for Proposals (RFP) in spring 2007, well before it issued its final rule on December 31, 2007 choosing vicinity RFID for the passport card.[29]**

- **DHS and the State Department remained committed to vicinity RFID despite Congress' *second* attempt to get the Departments to choose a secure machine-readable technology (this time for the EDL).** Section 7209(b)(1) of the IRTPA was amended a second time in August 2007 to direct the creation of an "enhanced driver's license" pilot program with a state, where the choice of machine-readable technology would be "based on individual privacy considerations and the costs and feasibility of incorporating any new technology into existing driver's licenses.''[30] In contravention of the clear Congressional intent, the State Department published its final rule confirming the vicinity RFID

---

[25] http://www.nist.gov/public_affairs/factsheet/whti.html

[26] *Supra* note 7.

[27] http://www.cdt.org/privacy/20060501rfid-best-practices.php

[28] Mr. Jeffrey wrote that "the Departments of State and Homeland Security reached agreement on the choice of the technology for the PASS Card which is called 'Gen 2 RFID' . . . [and so] NIST focused its efforts on working with the two agencies to assure that Gen 2 RFID met the requirements of Section 546," http://www.nist.gov/public_affairs/factsheet/baker_ltr_attachment.pdf.

[29] *See* Wade-Hahn Chan, "Controversial passport card system put out for bid," *Federal Computer Week* (June 1, 2007), http://www.fcw.com/online/news/102856-1.html. *See also* the Federal Business Opportunities website: https://www.fbo.gov/index?s=opportunity&mode=form&id=b292d52703e6d5d7f25baedf747e5530&tab=core&_cview=1.

[30] Section 723, Implementing Recommendations of the 9/11Commission Act of 2007, Public Law 110-53 (Aug. 3, 2007).

technology choice for the passport card on December 31, 2007, and DHS is currently working with states on their various vicinity-RFID enabled EDL programs.

- **DHS and the State Department have ignored public comments opposing vicinity RFID technology.** On October 17, 2006, the State Department solicited public comments in the Federal Register on its proposed choice of vicinity RFID technology for the passport card,[31] but it proceeded to ignore the bulk of the public comments, including those of experts.[32] By the State Department's own admission, the vast majority of the *over 4000 comments* opposed the vicinity RFID technology choice or the passport card itself. The State Department stated that only approximately "20 comments specifically voiced support for the passport card." **All four Members of Congress who commented, as well as technology, security, and privacy groups, expressed concern with the choice of vicinity RFID technology for the passport card. The State Department deflected this overwhelming public opposition by claiming that the opposition "reflected an improper understanding of the business model that WHTI is designed to meet and how the technology selected would actually be implemented."** The State Department also **failed to promulgate regulations addressing the privacy concerns** relating to how a citizen's unique ID number could be skimmed from the passport card and how databases associated with the card would be protected.

- Similarly, almost as an afterthought, DHS solicited public comments on the EDL in its proposed REAL ID regulations,[33] and confirmed in the *discussion* preceding the final regulations – despite much concern expressed in the public comments – that it was working with states to develop EDLs that are REAL ID-compliant and include vicinity RFID chips.[34] **But no regulations directing how the EDL program will be managed have been implemented by DHS.**

- **DHS has ignored the conclusion of its own Inspector General** who noted, in reviewing CBP's Trusted Traveler programs, that "[a]dditional security controls [such as encryption] would be required if CBP . . . migrates to universally readable Generation 2 (Gen2) products."[35]

---

[31] Department of State, *Card Format Passport; Changes to Passport Fee Schedule* (Proposed Rule), 71 Fed. Reg. 60928 (Oct. 17, 2006).

[32] Department of State, *Card Format Passport; Changes to Passport Fee Schedule* (Final Rule), 72 Fed. Reg. 74169 (Dec. 31, 2007) ("Passport Card Final Rule").

[33] Department of Homeland Security, *Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (Notice of Proposed Rulemaking), 72 Fed. Reg. 10820, 10841-42 (March 9, 2007).

[34] REAL ID Final Rule, *supra* note 16, at 5314 ("The use of RFID is essential to the WHTI program in order to ensure facilitation at crowded U.S. land and sea crossing points.").

[35] DHS IG Trusted Traveler Report, *supra* note 21, at 1, 7.

- **Program-specific Privacy Impact Assessments[36] have not been published for the passport card and EDL programs' use of vicinity RFID technology.** In January 2008, the DHS Privacy Office wrote a generic Privacy Impact Assessment on the use of vicinity RFID technology for land border crossings. While this PIA contains much valuable information and analysis, it noted that PIAs for the *specific* passport card and EDL programs, among others, "will be published prior to the programs' use of RFID technology to facilitate border crossing."[37] This has not happened. Washington State began issuing EDLs in January 2008 even though no EDL-specific PIA has been published by DHS. The State Department still has not issued a passport card-specific PIA[38] even though it has begun accepting applications and plans to begin issuing passport cards in June or July of this year.[39] CDT submitted a Freedom of Information Act request back in January 2007, and even wrote a letter to Secretary Rice in May 2007, requesting from the State Department a PIA for the passport card.[40] We never received a response.

- **Program-specific Systems of Record Notices (SORNs)[41] have not been published for the passport card and EDL programs' use of vicinity RFID technology.** In the State Department's latest SORN for "passport records" (Jan. 9, 2008), while the passport card is mentioned by name, there is no mention of the use of vicinity RFID technology and the fact

---

[36] Section 208(b)(1)(A) of the **E-Government Act of 2002**, Public Law 107-347 (Dec. 17, 2002), requires that an agency conduct a Privacy Impact Assessment "before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." Section 222 of the **Homeland Security Act of 2002**, Public Law 107-296, (Nov. 25, 2002), requires that DHS, specifically, conduct PIAs and that the Department use technologies that "sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." In addition to these statutes, the DHS Privacy Office directs the Department to conduct a PIA when it is **"developing or procuring any new technologies or systems that handle or collect personal information," such as "systems utilizing radio frequency identification devices (RFID)."** *Privacy Impact Assessments: Official Guidance*, at 11-12 (March 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_march_v5.pdf. Similarly, the Government Accountability Office stated, in relation to US-VISIT's inclusion of vicinity RFID chips in I-94 forms, that **"a privacy impact statement should be conducted before an agency develops or procures an information technology system, such as the proposed RFID system**, which collects, maintains, or disseminates information about an individual – in this case, numeric information that may be linked to biographic information contained within databases." *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248, at 81 (Dec. 2006) ("GAO US-VISIT Report"), http://www.gao.gov/new.items/d07248.pdf, *citing* Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB M-03-22 (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[37] DHS RFID PIA, *supra* note 4, at 2.

[38] List of State Department PIAs: http://www.state.gov/m/a/ips/c24223.htm.

[39] "U.S. Passport Card Frequently Asked Questions," http://travel.state.gov/passport/ppt_card/ppt_card_3921.html.

[40] http://www.cdt.org/security/identity/20070502rice.pdf

[41] Privacy Act of 1974, 5 U.S.C. §552a. The Privacy Act defines "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

that a unique ID number will be associated with each RFID chip and thus each citizen.[42] DHS apparently has not written a SORN for the EDL program even though CBP will be collecting the unique ID numbers of American travelers and directly accessing their associated personal information held in state databases.[43]

III. VICINITY RFID TECHNOLOGY IS UNNECESSARY AND THE OPERATIONAL BENEFITS ARE QUESTIONABLE

The first question that should be asked about any proposed ID program and the technology it will use is: *Is it necessary?* If the answer is "no" then the program should be scrapped or the technology should be changed, and the issue of privacy need not be reached. **In the case of the passport card and EDL, the answer to the question "is the use of vicinity RFID technology necessary?" is a resounding "no."**

It Does Not Appear That Vicinity RFID Will Be Any Faster Than Other Machine-Readable Technologies

DHS and the State Department defend the use of vicinity RFID technology in the passport card and EDL by claiming that it will enable faster processing of individuals at the border. Specifically, the Departments assert that the long read range (20-30 feet) of the vicinity RFID chip enables "pre-positioning" of a traveler's record, such that his or her personal information can be pulled up on CBP computers and checked against terrorist watchlists and law enforcement databases before the traveler reaches the CBP officer at the inspection booth. Thus, the Departments argue, vicinity RFID technology is necessary to move travelers through primary inspection more quickly.[44] The truth of this assertion is not apparent.

DHS and the State Department fail to acknowledge that "pre-positioning" can be achieved with other machine-readable technologies. Rather than using vicinity RFID chips that can be read from 20 feet away, card readers can be placed 20 feet from the inspection booth and another more secure machine-readable technology can be used that will *minimize the risk of the citizen's unique ID number being surreptitiously skimmed by a rogue reader from afar.* Such technologies include a barcode, magnetic stripe, or even "proximity" or short-range RFID that can be read from no more than a few millimeters away. **In fact, the EDLs are already being designed with two "machine-readable zones," the vicinity RFID chip *and a second MRZ*, so "that the CBP officer can read [the card] electronically if [an] RFID [reader] isn't available."[45]** (However, as mentioned above, even with other MRZ technologies, there is still the question of whether the citizen's unique ID number is encrypted or otherwise secured from unauthorized access.)

---

[42] http://www.state.gov/documents/organization/102790.pdf

[43] List of DHS SORNS: http://www.dhs.gov/xinfoshare/publications/gc_1185458955781.shtm.

[44] DHS RFID PIA, *supra* note 4, at 3.

[45] Department of Homeland Security, "Enhanced Drivers Licenses: What Are They?", http://www.dhs.gov/xtrvlsec/crossingborders/gc_1197575704846.shtm.

The Departments also claim that vicinity RFID technology is necessary to read multiple cards at one time, which they assert will also significantly decrease primary inspection times.[46] This claim seems very dubious. While vicinity RFID does have the capability to read multiple cards at the same time, it will be wasted in the border crossing context. The CBP officer must still compare the traveler, the picture on the card, and the database information *one person at a time*. **Any time gained in scanning a carload of passport cards or EDLs simultaneously will be lost due to the need to process each traveler individually, comparing each card with the holder *and* the stored record to make sure no one is using a stolen card.** Moreover, past evidence has suggested that **read rates of vicinity RFID chips can be poor.**[47]

DHS Has Not Disclosed Any Studies Favorably Comparing Vicinity RFID With Other Technologies

DHS has consistently asserted that vicinity RFID is the best technology to enable both pre-positioning and faster processing of individuals at the border. On April 16, 2008, before the House Homeland Security Committee, Subcommittee on Border, Maritime and Global Counterterrorism, DHS representatives testified that "After extensive review of available and even possible technologies, DHS selected vicinity RFID as the best technology for our land border management system."[48] However, what is curious about DHS' April 16 testimony is that while the Department "reviewed" other possible machine-readable technologies, **DHS representatives did *not* testify that that the Department conducted timing or efficiency studies *comparing* vicinity RFID to other machine-readable technologies that also allow for pre-positioning of traveler information.** DHS simply testified, "Our research and testing indicates that RFID technology is *able* to accomplish" the Department's goals, and that "the introduction of *RFID enabled* documents significantly reduced primary processing time."[49]

Even if vicinity RFID did outperform other technologies in terms of improving traveler processing time, DHS and the State Department should not have chosen vicinity RFID technology without also considering the risks to *privacy*: that is, comparing the risks posed by vicinity RFID against any privacy risks posed by other technologies. In CDT's January 2007 comments to the State Department on the proposed technology choice for the passport card, we expressly called for in-field testing of machine-readable technologies that objectively weighed privacy and security risks against any identified benefits such as increased efficiency.[50]

Our recommendation was consistent with the recommendation of DHS's own Data Privacy & Integrity Advisory Committee:

---

[46] Passport Card Final Rule, *supra* note 32, at 74170.

[47] GAO US-VISIT Report, *supra* note 36, at 48, 54 ("the US-VISIT Program Office reported that the exit read rates that occurred during the test generally fell short of the expected target rates for both pedestrians and for travelers in vehicles").

[48] http://homeland.house.gov/SiteDocuments/20080416142622-93835.pdf (p. 10).

[49] *Supra* note 48 (p. 11) (emphasis added).

[50] http://www.cdt.org/security/20070108passcard.pdf (p. 20).

> Before deploying any technology, the Department should define the program *objective*, determine what technologies may apply, and understand the benefits and concerns related to each deployment. With that as background, there needs to be an analysis of what is the *least intrusive technology* that can be used to accomplish the objectives of the program and what technologies can be used to help address any privacy concerns that exist.[51]

DHS and the State Department have failed to conduct such a cost-benefit analysis.

The Compatibility Argument Has No Merit

Finally, DHS and the State Department defend the choice of vicinity RFID technology by arguing that it will "ensure compatibility and interoperability with the DHS border management system."[52] **Yet the Departments seem to have forgotten that CBP must be able to read the new electronic passport at the borders, which has a different technical architecture than the passport card and EDL.** Moreover, the Trusted Traveler programs that do use vicinity RFID technology have been using first generation (Gen 1) chips, which also require a different reader system.[53] Thus the Departments' compatibility argument has no merit.

The Differences Between the Electronic Passport and the Passport Card/EDL Are Telling

All of the necessity, efficiency and compatibility arguments cited by the government in support of vicinity RFID are undercut by the fact that the electronic passport has many more privacy and security features than the passport card and EDL, even though all three documents are meant to serve the same function – prove U.S. citizenship so that an individual can re-enter the country. Key differences between the e-passport's and the passport card/EDL's security features include:

e-Passport Security Features	Passport Card/Enhanced Driver's License Security Features
• Short-range ("proximity-read") radio-frequency (RF) wireless chip (approx. 3 inches) • Holds same personal identification information as on main page of passport book, including digital photograph to be used with facial recognition technology at the border (currently visual inspection	• Long-range ("vicinity-read") radio-frequency (RF) wireless chip (approx. 20 – 30 feet, and possibly much more) • Stores unique ID number that corresponds to computer file with personal identification information in government database; no personal identification information is on the chip

[51] DHS Privacy Committee RFID Report, *supra* note 7, at 2 (emphasis added).

[52] Passport Card Final Rule, *supra* note 32, at 74170.

[53] DHS IG Trusted Traveler Report, *supra* note 21, at 3 ("Generation 1 tags use proprietary technology, which means that if Company A puts an RFID tag on a product it cannot be read by Company B unless both use the same RFID system supplied from the same vendor.").

only) • Digital signature to verify that personal identification information on chip is authentic • Basic Access Control (BAC) technology locks/unlocks chip; passport must be physically swiped (contact communication) and cryptographic keys stored on passport book are used to unlock the chip and enable it to communicate wirelessly (contact less communication) • Even if BAC cannot be bypassed, a rogue reader attempting to detect a signal will be presented with a different random number on each try, **therefore providing no unique ID number to enable tracking** • Personal identification information encrypted while stored on the chip (at rest) • Personal identification information encrypted during RF wireless (contactless) communication (during transmission) • RF shielding (metal) incorporated into passport book to block RF signals when book is closed	• Protective sleeve to block RF signals offered to citizens (voluntary)

CONCLUSION: CONGRESSIONAL ACTION IS NEEDED TO PROTECT PRIVACY AND SECURITY

CDT takes no position on the value of the Western Hemisphere Travel Initiative, specifically, the requirement that American citizens present a passport or equivalent document when seeking to re-enter the United States at the land borders. Nor do we find unreasonable Congress' desire to minimize congestion at the land borders due to this new requirement, in part, by ensuring that frequent cross-border travelers can be processed relatively quickly so that CBP officers can focus the bulk of their efforts on inspecting the rest of the travelers.

However, these two policy objectives do *not* necessitate the use of insecure vicinity RFID technology in human identification documents. As discussed above, such an application of this technology:

- Poses clear and serious risks to personal privacy and security;
- Disregards concerns expressed by both Congress and the public; and
- Affords no clear operational benefits in the border crossing context.

CDT concludes that the use of vicinity RFID technology in human identification documents, such as the passport card and EDL, is inappropriate at this time due to the lack of meaningful security measures. CDT is also concerned with the potential uses of the REAL ID card, the passport card and the EDL to facilitate tracking of the movements and activities of Americans in contexts having nothing to do with highway safety, border control or airline passenger screening. The less secure the ID number and other information is on these documents, the more likely it is that the cards will be used by governmental and commercial entities to compile databases that can be used to track and profile citizens. **To address both the problem of unauthorized skimming or interception, and the risk that the cards will be used to facilitate creation of governmental or commercial databases, we urge Congress to direct DHS and the State Department to use machine-readable technologies in the passport card and EDL that provide privacy protections commensurate with those in the electronic passport.**

Thank you for the opportunity to testify before the Subcommittee. CDT is eager to work with the Subcommittee and the Administration to develop documents for use in border crossings that enhance national security and protect personal privacy and security.

APPENDIX

http://www.cdt.org/security/identity/20080201_REAL ID_hillbrief.pdf

February 1, 2008

REAL ID: WHAT SHOULD CONGRESS DO NOW?
CDT Analysis of the REAL ID Act and the Department of Homeland Security's Final Regulations

I. SUMMARY ANALYSIS OF FINAL REAL ID REGULATIONS

The Department of Homeland Security's final regulations have rendered REAL ID virtually useless as a security measure, while still posing serious privacy problems. States balked at reforms that might have actually made driver's license issuance more secure and DHS capitulated. For example, DHS:

- Failed to create specific and detailed minimum security standards for the physical design of the REAL ID cards to thwart tampering and counterfeiting [Preamble pp. 29, 131];[1]
- Failed to create specific and detailed minimum security standards for the protection of physical facilities where cards are made and supplies are stored [Preamble pp. 154-156]; and
- Failed to mandate central issuance of driver's licenses and ID cards at the state level, which would have helped combat insider fraud at local DMV offices [Preamble p. 156].

Under the final regulations, the REAL ID program will not do much beyond what states are already doing. DHS deferred to the status quo. For example, DHS:

- Expressed implied deference to AAMVA's[2] Driver Licensing/Identification Card Design Specification [Preamble p. 131];
- Approved use of AAMVA's training program on fraudulent document recognition, which the majority of states currently use [Preamble p. 169];
- Mandated use of the two-dimensional barcode, which is already being used by 45 jurisdictions [Preamble p. 141]; and
- Mandated that states electronically verify Social Security Numbers, which 47 states already do via AAMVA's network [Preamble p. 19].

---

[1] Preamble page numbers refer to the version of the REAL ID final regulations published on the Department of Homeland Security's website on January 11, 2008, http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part1_2008-01-11.pdf; http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part2_2008-01-11.pdf.

[2] American Association of Motor Vehicle Administrators, http://www.aamva.org/.

Perhaps the only meaningful REAL ID reform measure is the requirement that states electronically verify source documents presented by individuals to prove identity and lawful presence in the United States. However, while 47 states currently verify SSNs with the Social Security Administration, as DHS explains, "verification of birth certificates is limited to those States whose vital events records are available online." Other systems to enable states to confirm an individual's legal status have not been developed (such as the link to the State Department's passport database) or are not fully operational (such as the database to verify legal immigrants). [Preamble p. 19]

Not only will REAL ID be ineffective at making driver's license issuance more secure and the card a more reliable assertion of identity, REAL ID also creates new privacy and security risks while exacerbating existing ones. Several states have already indicated that they will not follow the program precisely because of the significant threats to civil liberties.[3]

CDT has five specific criticisms of the REAL ID program (as defined by the Act and the final regulations), focusing on risks to personal privacy and security:

1. **The REAL ID card will become a *de facto* national ID card.**

2. **REAL ID will likely result in the creation of a central ID database, which will threaten the privacy and security of 240 million Americans.**

3. **DHS is mandating a standardized and unencrypted Machine-Readable Zone (MRZ), which will facilitate intrusive tracking by both government and commercial entities.**

4. **DHS failed to adopt meaningful privacy and security standards for the protection of personal information in the REAL ID system.**

5. **In a related initiative, DHS is creating driver's licenses with imbedded, insecure RFID chips (Enhanced Driver's Licenses) that will threaten the personal privacy and security of American citizens, without Congressional oversight or an administrative rulemaking.**

[3] *See* ACLU's website on REAL ID: http://www.realnightmare.org/news/105/.

II. FIVE SIGNIFICANT PRIVACY AND SECURITY RISKS STILL LOOM

1. The REAL ID card will become a *de facto* national ID card.

> *"The term 'official purpose' includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine." [REAL ID Act §201(3)]*

- **DHS has retained *unfettered discretion* to expand the definition of "official purpose" and thus the contexts in which the card can be required.** While CDT is pleased that DHS has, for now, limited the definition of "official purpose" to those specifically enumerated in the statute [Final Rule §37.03], CDT is concerned that DHS can require a REAL ID for variety of other purposes, and will do so without prior Congressional approval or public input via an administrative notice and comment procedure.[4]
- While DHS asserts that it does not support the creation of a national ID card [Preamble pp. 80, 92], the Department at the same time states that it *"will continue to consider additional ways in which a REAL ID license can or should be used and will implement any changes to the definition of 'official purpose' or determinations regarding additional uses for REAL ID consistent with applicable laws and regulatory requirements. DHS does not agree that it must seek the approval of Congress . . . as §201(3) of the Act gives discretion to the Secretary of Homeland Security to determine other purposes."* [Preamble p. 69]
- Moreover, there is no limit on the permissible uses of the REAL ID card by governmental or commercial entities and DHS states that it has neither the power nor any interest in limiting such uses.[5] Merchants and others are free to ask for the card and to collect data from it. There is a very real possibility that **individuals will not be able function in U.S. society without a REAL ID card.**
- **Using a single ID card for multiple purposes is bad for security.** It is ironic that REAL ID moves the nation closer toward a national ID card while Congress and the federal agencies have been striving to reduce the use of the Social Security Number, which has been the de facto national identifier and a key facilitator of ID theft.
- **There is a very high risk of "mission creep" with respect to REAL ID.** Just five days after the final regulations were published on the DHS website, a senior Department policy official publicly suggested that REAL ID could help fight the methamphetamine crisis.[6] This follows Congressional proposals to require a REAL ID card for a myriad of different purposes including employment, federal housing benefits, and voting.

---

[4] CDT commends DHS, however, for not mandating that REAL ID card numbers be unique across states. [Preamble p. 30]

[5] DHS washes its hands of this issue: *"DHS does not intend that a REAL ID document become a de facto national ID based on the actions of others outside of DHS to limit their acceptance of an identity document to a REAL ID-compliant driver's license or identification card."* [Preamble p. 69]

[6] Anne Broache, "DHS: Real ID could help shut down meth labs," *CNET news.com,* http://www.news.com/8301-10784_3-9851813-7.html?tag=bl.

2. REAL ID will likely result in the creation of a central ID database, which will threaten the privacy and security of 240 million Americans.

Each state shall:

"Provide electronic access to all other States to information contained in the motor vehicle database of the State." [REAL ID Act §202(d)(12)]

"Refuse to issue a driver's license or identification card to a person holding a driver's license issued by another State without confirmation that the person is terminating or has terminated the driver's license." [REAL ID Act §202(d)(6)]

- In direct contradiction of the claims of DHS Secretary Chertoff that *"We are not going to have a national database,"*[7] the final regulations reject a decentralized approach and make it clear that **DHS expects that REAL ID implementation will require the creation of a central "hub" for information exchange among the states [Preamble pp. 18-20, 80-84, 90] and/or a central database of identifying information.** No comfort can be taken from the failure of DHS to clearly define the nature of the centralized features of REAL ID implementation; to the contrary, a key aspect of REAL ID implementation may be developed without public notice or input.
- For the central database, DHS prefers expanding the centralized Commercial Driver's License Information System (CDLIS) to include all driver's license and ID card holders.[8] DHS fails to acknowledge **the serious privacy and security risks of creating a central ID database on 240 million Americans** [Preamble p. 15], which is a far cry from the 13 million commercial drivers whose identity information is currently stored in the CDLIS system.
- **There is no robust legal framework that would ensure the security and protect the privacy of the personal information stored in a central ID database.** DHS is planning to rely on a non-governmental organization, the American Association of Motor Vehicle Administrators,[9] or some other non-governmental entity to create the information exchange hub and the centralized pointer system or other centralized database for REAL ID implementation. DHS admits that the security and privacy rules for the personal data held by AAMVA are solely the creation of that nonprofit organization: *"AAMVAnet is governed by the Board of AAMVA and it subject to the security and privacy requirements established by the association of DMVs."* [Preamble p. 93]

---

[7] Remarks by Homeland Security Secretary Michael Chertoff at a Press Conference on REAL ID (Jan. 11, 2008), http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm.

[8] The CDLIS central ID database holds key identifying information on commercial drivers such as name, date of birth, and Social Security Number, and this record links or "points" to the individual's commercial driving history that is housed in the motor vehicle database of the state that issued the commercial driver's license. http://www.aamva.org/TechServices/AppServ/CDLIS/

[9] These comments are in no way a criticism of AAMVA. Starting well before REAL ID, and without pressure or support from the federal government, AAMVA and its members have taken major steps to improve the security of the driver's license issuance process. AAMVA has been one of the most credible voices of reason throughout the REAL ID process.

- Regarding security, **it would be a major error to store the personal information of millions of Americans in a central location**. Security experts agree that centrally storing (or even making centrally accessible via linked databases) highly valuable data would create a treasure trove for identity thieves, terrorists, and unscrupulous government employees.[10] Data stored in the CDLIS central database, as well as data in transit, is not even currently encrypted.[11]
- DHS asserts that there is a security benefit to AAMVA's network ("AAMVAnet") being a private network. [Preamble pp. 18, 82]. However, even **private networks are vulnerable to attack** by sophisticated hackers and identity thieves who are not daunted by a private network's lack of connection to the public Internet. This is especially true if the network carries information as valuable as the personal details on hundreds of millions of Americans. And the fact that the network may be private has no bearing on the risk for internal abuse, which is a leading source of driver's license fraud and identity theft.[12]
- The **Privacy Act** likely would not apply to a driver's license database managed by a private entity such as AAMVA, which currently runs the CDLIS database. Nor would the **Driver's Privacy Protection Act** provide adequate privacy protections for personal information in such a database.[13]
- The final regulations do not limit **government access** to information held in any kind of central ID system that might be created under REAL ID. To the contrary, DHS asserts that the database would be accessed not only by federal officials involved in highway and motor vehicle safety but also by federal officials involved in law enforcement and **"the verification of personal identity."** [Preamble pp. 83-84]
- To ensure "one driver, one license," CDT has recommended building a **true distributed system that stores ID information locally**, in state motor vehicle databases. Each state could check with other states for possible existing driver's licenses without having to ping a central database, while maintaining control over its residents' data. This is technologically possible, especially if states have adequate funding to scale up their systems to handle the incoming traffic.

---

[10] Bruce Schneier, "REAL-ID: Costs and Benefits" (Jan. 30, 2007), http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html.

[11] Personal data stored in the CDLIS central database is in unencrypted form, as is personal information transmitted via the CDLIS network. AAMVA has begun to encrypt both the static and dynamic CDLIS data. However, the Federal Register notice related to CDLIS modernization 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.

[12] *See* Ari Schwartz, "Unlicensed Fraud: How Bribery and Lax Security at State Motor Vehicle Offices Nationwide Lead to Identity Theft and Illegal Driver's Licenses" (Feb. 2004), http://www.cdt.org/privacy/20040200dmv.pdf. *See also* Jon Stokes, "Analysis: Metcalfe's Law + Real ID = more crime, less safety," *Ars Technica* (Jan. 19, 2008), http://arstechnica.com/news.ars/post/20080119-analysis-metcalfes-law-real-id-more-crime-less-safety.html.

[13] 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*.

- DHS claims that *"State systems would not be able to handle the volume of messages received if all jurisdictions were sending and receiving messages from all jurisdictions at the same time"* in a true distributed system. [Preamble p. 83] Yet DHS has not conducted a detailed analysis proving this point nor determining what would be involved if state systems were scaled up to handle the traffic generated by a true distributed system. DHS has failed to answer key questions:
    - How many **queries** (requests and responses) will each state have to handle? This presumably can be determined if we know how many new DL/ID applications each state receives on average each year.
    - What would be the **bandwidth load or amount of data** each state would have to handle? Presumably this would be the same for all states: the personal information fields needed to uniquely identify an individual.
    - What is the nature of existing state motor vehicle department infrastructures (i.e., baseline conditions)? Specifically, a) what is the **computing power** of their servers, and b) what is their **network capacity** (i.e., bandwidth)?
    - How much **upgrading** will be needed for each state motor vehicle department (based on their existing/baseline systems)? How much will this **cost?**
- **The final regulations do not limit what information will go into the centralized database and do not prohibit the collection and storage of additional information on individuals.** We must not create the technological architecture that will open the door wide open to future abuse, including the tracking of individuals and the creation of national dossiers American citizens.

3. DHS is mandating a standardized and unencrypted Machine-Readable Zone (MRZ), which will facilitate intrusive tracking by both government and commercial entities.

Each REAL ID driver's license or identification card shall include "A common machine-readable technology, with defined minimum data elements." [REAL ID Act §202(b)(9]

- While DHS has chosen the relatively benign two-dimensional bar code as the standard for the MRZ, a fundamental problem is that the Act requires that the MRZ must be **standardized** across jurisdictions. This will increase the likelihood that the private sector will adopt "skimming" technologies that facilitate capture and storage of information from the card as it is used in ordinary commercial activities.
- The final regulations **do not require encryption or other security measures** to inhibit the scanning of the MRZ and the collection or "skimming" of personal information [Final Rule §37.19], even though three commenting states supported encryption [Preamble p. 142].
- DHS also implies that encryption is for the time being *prohibited*: *"If, in the future, the States collectively determine that it is feasible to introduce encryption, DHS may consider such an effort so long as the encryption program enables law enforcement easy access to the information in the MRZ."* [Preamble p. 86, 144]
- **The final regulations do not prevent innumerable state and federal agencies, as well as businesses and non-governmental third parties, from scanning the MRZ, collecting personal information and recording individual's activities.** The final regulations do not limit those who may scan the MRZ to only *state motor vehicle officials for legitimate*

administrative purposes and law enforcement officials for legitimate law enforcement purposes.

- The REAL ID Act does not address security of the MRZ, but the Conference Report explicitly contemplates that personal data would be "stored securely and only able to be read by law enforcement officials."[14]
- DHS punts to the states the issue of prohibiting others from using the MRZ: *"DHS strongly encourages the States to address concerns about the ability of non-law enforcement third-parties to collect or skim personal information stored on the REAL ID driver's licenses or identification cards."* [Preamble p. 86]
- DHS also sidesteps the issue of limiting federal use of the MRZ by stating that the Department is *"not aware of any current plans by Federal agencies to collect and maintain any of the information stored in the MRZ," but should they "want to use the MRZ to collect and maintain personally identifiable information in the future, any such information . . . would be subject to the protections of the Privacy Act . . . ."* [Preamble pp. 87, 138]The Privacy Act, however, gives federal agencies broad latitude to collect, store and exchange information.

- The final regulations **do not limit what personal information may be stored in the MRZ.** [Final Rule §37.19] DHS acknowledges that the final regulations set *"the minimum elements to include [in the MRZ], but recognizes the authority of the individual States to add other elements such as biometrics, which some currently include in their cards."* [Preamble p. 140]
- Taken together, the MRZ mandate, the standardization of the MRZ technology, the lack of encryption or other security requirements, and the lack of use and collection limitations mean that the REAL ID card will **facilitate government and commercial surveillance of American citizens.**

4. DHS failed to adopt meaningful privacy and security standards for the protection of personal information in the REAL ID system.

Each state shall "Employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format." [REAL ID Act §202(d)(1)]

Each state shall "Retain paper copies of source documents for a minimum of 7 years or images of source documents presented for a minimum of 10 years." [REAL ID Act §202(d)(2)]

Each driver's license and identification card shall include "Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes." [REAL ID Act §202(b)(8)]

Each state shall "Ensure the physical security of locations where drivers' [sic] *licenses and identification cards are produced and the security of document materials and papers from which drivers' licenses* [sic] *and identification cards are produced." [REAL ID Act §202(d)(7)]*

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

- **The REAL ID Act itself does not require that personal information, including source documents, collected and stored pursuant to the Act be protected by privacy and security safeguards.** CDT is pleased that DHS has interpreted its authority to include the power to require states to develop a privacy policy as well as institute "Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of [] personally identifiable information." [Final Rule §37.41, §37.43] CDT is also pleased that state privacy laws are not preempted [Preamble p. 51] and that DMVs can record birth certificate information in lieu of copying the document, which aims "to protect medical and other personal information not relevant to REAL ID" [Preamble p. 34].
- However, **the final regulations say nothing about what must be in state privacy policies and the required "Security Plan." [Final Rule §37.41(b)(2)(ii)]** DHS claims that the **privacy policy** should follow the Fair Information Principles [FIPs], but fails to require this in the final regulations. [Preamble p. 85] **The final regulations fail to include specific privacy and security standards against which DHS will determine states' "compliance" with the REAL ID Act.**
- DHS provided no meaningful response to comments that the Security Plans should be evaluated against specific minimum standards. In response to the comment that DHS should "create stronger protections for information to limit the danger of aggregating information on 240 million Americans," DHS stated simply that at some point in the future it will work *"to develop best practices for risk and vulnerability assessments as well as for security plans for DMV facilities."* [Preamble pp. 156-159] It is unclear why DHS did not do this in the REAL ID final rule that was just published.
- While the final regulations provide that "Any release or use of personal information collected and maintained by the DMV pursuant to the REAL ID Act must comply with the requirements of the Driver's Privacy Protections Act" [Final Rule §37.41(b)(2)(iii)] [Preamble p. 35], it is clear that the DPPA would have applied *anyway* to personal information collected and stored by state motor vehicle departments pursuant to the REAL ID Act. So this provision in the final rule adds no privacy protection not already provided by law.
- Moreover, as discussed above, **the DPPA offers incomplete protection of personal privacy (it includes many exceptions that virtually swallow the main non-disclosure rule[15]).** DHS admits that *"Although the DPPA provides for a large number of permissible uses, it is the only Federal law that currently applies to State DMV records and will provide a floor that States can build upon to further limit the disclosure of DMV record information."* [Preamble p. 85]
- As discussed above, the final regulations do not prohibit federal and state government agencies, businesses, and other third-parties from **accessing personal information** that might be stored in a central ID database or in the MRZ.

[15] "DHS cannot rely on the [Driver's Privacy Protection Act] to protect the privacy of the personal information required under the REAL ID Act." The DPPA "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." DHS Privacy Office, *Privacy Impact Assessment for the REAL ID Act*, at 12 (March 1, 2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf.

- The DHS Privacy Office wrote a helpful set of **"best practices,"** but these are voluntary, not mandatory.[16]

5. In a related initiative, DHS is creating driver's licenses with imbedded, insecure RFID chips (Enhanced Driver's Licenses) that will threaten the personal privacy and security of American citizens, without Congressional oversight and an administrative rulemaking.

- While not part of the final REAL ID regulations, DHS solicited comments on – and is moving ahead with – creating a REAL ID-compliant driver's license that U.S. citizens can use for crossing the land borders. [Preamble pp. 22-23, 172-178] The so-called "Enhanced Driver's License" (EDL) would have **a long-range (or "vicinity-read") RFID chip, which is an insecure technology and inappropriate for human identification.**[17]
- **The RFID chip will threaten personal privacy and security by enabling tracking of individuals.**[18] While no personal information will be stored on the RFID chip, a unique and static identification number will be stored without encryption on the chip, enabling anyone with a compatible and widely available reader to skim the number and use it as the basis for an identification system.
- **Personal privacy will also be at risk because the EDL program will enable the consolidation of personal information: the federal government will have direct access to state DMV records, and state DMVs may be able to record individuals' travel histories.** Rather than having the unique identification number on the RFID chip correspond with a record in a State Department database that confirms the person's U.S. citizenship, DHS is proposing that the ID number allow Customs & Border Protection (CBP) to connect directly to the state motor vehicle database.[19]
- U.S. citizenship will be denoted on the face of the license [Preamble p. 23], which could lead to **discrimination** against cardholders who do not have a U.S. citizenship mark. [Preamble p. 173]
- The Department of State is moving ahead with a similar "passport card" program despite having received thousands of comments, the **majority of which *opposed* the RFID technology choice.**[20]

---

[16] DHS Privacy Office, *Privacy Impact Assessment for the REAL ID Final Rule*, Attachment A (Jan. 11, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realidfr.pdf.

[17] *See* DHS Data Privacy and Integrity Advisory Committee, *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.

[18] Even the State Department recognizes there is a threat of surreptitious scanning of the card and tracking of American citizens. Passport Card FAQs, http://travel.state.gov/passport/ppt_card/ppt_card_3921.html.

[19] *See, e.g.*, Vermont EDL fact sheet, http://www.dmv.state.vt.us/documents/MiscellaneousDocuments/EnhancedDriverLicenseAndIDCard.pdf.

[20] Card Format Passport; Changes to Passport Fee Schedule, Final Rule, 72 Fed. Reg. 74170 (Jan. 31, 2007).

III. CDT SUPPORTS THREE LEGISLATIVE OPTIONS

In writing weak final regulations to implement REAL ID, DHS followed the lead of Congress, which failed to include privacy and security requirements in the REAL ID Act. The *current* Congress must revisit driver's license reform and pass legislation that will in fact make driver's licenses more reliable IDs without posing serious threats to individual rights.

OPTION 1: Repeal REAL ID & Replace With a Negotiated Rulemaking and Privacy/Security Mandates [S. 717]

CDT has consistently supported the Identification Security Enhancement Act of 2007 [S. 717], introduced by Senators Akaka, Sununu, Leahy and Tester in February of last year.

This bill would repeal Title II of the REAL ID Act and replace it with a **negotiated rulemaking committee** and language specifically addressing **privacy and civil liberties**. The goal is to go back to the process originally called for by §7212 of the Intelligence Reform and Terrorism Prevention Act of 2004, which REAL ID repealed in 2005.

A negotiated rulemaking committee could:

- Develop meaningful federal minimum standards that would actually make driver's license issuance more secure and the card a more reliable assertion of identity;
- Write regulations that would have the backing of all relevant stakeholders, including the various states (including, hopefully, the 17 states that have vowed *not* to implement REAL ID) and individual rights advocates;
- Still promote implementation of reforms on a schedule faster than what DHS proposes for REAL ID.

OPTION 2: Amend REAL ID to Address Specific Privacy and Security Risks

If "repeal" is not possible, Congress should, at a minimum, fill the huge privacy and security gaps created by REAL ID. Suggestions include:

- Amend the REAL ID Act to prohibit expanded required uses of the REAL ID card and to include statutory language that specifically prohibits card numbers from being unique across the nation.
- Delete the "electronic access" provision of the REAL ID Act, §202(d)(12), and prohibit the creation of a central ID database, either managed by the government or a private entity.
- Repeal the mandate for a standardized Machine Readable Zone.
- To the extent that states wish to include an MRZ on driver's licenses and ID cards, mandate encryption and/or other security features.
- To the extent that states wish to include an MRZ on driver's licenses and ID cards, mandate that states include no more than a specified maximum number of personal data elements.

- To the extent that states wish to include an MRZ on driver's licenses and ID cards, prohibit state and federal agencies, and businesses and other private organizations, from scanning the card to collect personal information or track individuals' activities.
- Mandate specific privacy and security standards for the protection of personal information stored in computer systems and on the card itself (including deleting the requirement that states retain copies of source documents). This should also include amending the **Driver's Privacy Protection Act (DPPA). Among other things, the Act should be amended to clearly address the issue of personal ID information managed by a private entity such as AAMVA.**
- Prohibit the use of long-range RFID technology (or similarly insecure technology) in driver's licenses/ID cards, or at least create a structure that enables Congressional oversight of such a program.
- Reassess the Enhanced Driver's License program, including the proposed structure enabling CBP to connect to state databases and possibly enabling states to record residents' travel histories.
- Order an administrative rulemaking, with public notice and comment, to determine how state driver's licenses and ID cards can best be designed to enable land border crossings.

OPTION 3: Repeal REAL ID & Replace With a Simplified Law That Focuses on Source Document Verification

REAL ID's attempt at driver's license reform is an unfunded mandate that is a "stick" rather than a "carrot." In new legislation, Congress could:

- Change how it exercises authority over the states, from invoking the right to regulate IDs used for federal purposes to **conditioning federal monies on states taking certain driver's license reform actions.** This would create a financial incentive (a "carrot") for all states to follow the same minimum standards to make driver's license/ID card issuance more secure.
- Specify that **verification of source documents** is the primary minimum requirement to receive federal money. Arguably the most meaningful thing REAL ID does is to require states to verify identity and legal status against federal databases. Congress should provide federal money and a clear directive to the relevant federal agencies to expand source document electronic verification systems. **This singular focus would go a long way at making driver's licenses and ID cards more reliable identification credentials.**
- And, as suggested above, mandate specific privacy and security standards for the protection of personal information, which could be in the form of amendments to the **Driver's Privacy Protection Act (DPPA)**.

For more information contact:

Sophia Cope, Staff Attorney
Center for Democracy & Technology
scope@cdt.org
202-637-9800 x104

Additional materials on REAL ID can be found at: http://www.cdt.org/security/identity/

###