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

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];

---

[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/.

- 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].

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)]

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

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)]*

- **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*

[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.

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.
- 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]

---

[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.

- 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]

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.

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

- 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/