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

July 25, 2007

Dear Senator:

We encourage you to vote NO on an amendment to the Homeland Security Appropriations Bill (S. 1644) that Senators Alexander and Collins are expected to offer this week to provide $300 million in funding for the states to implement the REAL ID Act.

**No amount of federal funding can fix the fundamental flaws in the REAL ID Act. The Act has serious privacy and security problems that can be fully addressed only by rewriting the Act.**

**Before money is spent implementing REAL ID, the Act should be rewritten.** A strong starting point is the **Identification Security Enhancement Act of 2007 (S. 717).** But Congress must act soon. The Department of Homeland Security is moving forward to develop regulations to implement the Act in its flawed form. Once the regulations are finalized, it may become harder to address the privacy and security gaps in the original statute.

In its currently flawed form, lacking robust privacy and security protections, REAL ID cannot be effective in meeting its stated policy goals of combating terrorism and ID theft. Indeed, in its flawed state, REAL ID is likely to create security and ID theft problems rather than solve them. **Before funds are appropriated and expended, Congress should rewrite the Act to promote meaningful driver's license reform, which requires a strong privacy and security framework.**

The privacy and security concerns with REAL ID primarily stem from how personal information would be stored in databases and on the card itself, and who would have access to that data and for what purposes.

Under DHS's proposed regulation, REAL ID would result in the creation of a networked system containing the personal data of all driver's license and ID card holders (in other words, of virtually every American), **without** specific, robust privacy and security standards. REAL ID would thus create a highly valuable store of personal data (including highly sensitive source documents such as birth certificates, Social Security Cards, and passports, which REAL ID requires states to scan and store digitally). This information would be vulnerable to terrorists, ID thieves, and unscrupulous DMV or other government employees seeking to steal identities or do other harm. These concerns apply equally whether the data is centralized or resides in a system of linked DMV databases without proper safeguards.

REAL ID also mandates that each card contain a machine-readable zone (MRZ), which DHS will likely mandate be standard across all states. The MRZ mandate was intended to aid law enforcement in processing suspects with greater accuracy and efficiency. However, the standardized technology, along with the absence of use limitations and an encryption requirement, will create a serious risk that government agencies and commercial entities will scan the MRZ to log a multitude of public and private transactions having nothing to do with driver safety, law enforcement or national security. The MRZ as proposed would facilitate creation of a comprehensive digital record of citizens' travels and purchases that could be used for both government surveillance and unwanted solicitation.

CDT encourages the Senate to reject any spending on REAL ID implementation until the Act has been fundamentally rewritten to establish a meaningful driver's license reform program that respects privacy and ensures the security of personal information.

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