PREPARED ORAL STATEMENT OF SOPHIA COPE

Staff Attorney/Ron Plesser Fellow, Center for Democracy & Technology
Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
"The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative"
April 29, 2008

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

CDT has significant concerns with both REAL ID and WHTI. In the few minutes I have here today, I will focus on WHTI. However, both initiatives pose serious risks to the rights of American citizens and Congressional action is needed now.

CDT takes no position on the requirement that American citizens must now 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 border due to this new requirement.

The problem is that DHS and the State Department have chosen an insecure technology – vicinity RFID – for the passport card and Enhanced Driver's License.

Also, the Departments have not given any serious consideration to the risks to personal privacy and security posed by the use of this technology, despite concerns raised in thousands of public comments, two pieces of federal legislation, and by DHS' own Inspector General.

Additionally, it is not clear why the Departments chose vicinity RFID. It does not provide unique operational benefits in the border crossing context. And there is already a secure infrastructure in place for the electronic passport, which makes sense to use here.

I would like to make two main points, and then offer some recommendations.

First: Vicinity RFID technology is insecure and inappropriate for human identification.

This technology was NOT created to identify people. Rather, it was intended to track things – like televisions, toothpaste, and toilet paper. It was designed to be quickly and easily scanned by standardized readers, unencumbered by security features, as products move through the supply chain.

- Sensitive information on the RFID chip can be picked up by unauthorized people because it is stored and transmitted unencrypted and in the clear.
- The information can be read by any reader compatible with a common standard.
- And third, these readers can secretly read the vicinity RFID chip remotely from distances of 30 feet – and potentially many times more than that.

Second: The risks to privacy here are real.

For example, the "unique ID number" on the RFID chip will, overtime, become yet another identifier that can be used to track and profile the movements and activities of innocent Americans. Many citizens will likely not use a protective sleeve. Even those who do will likely take their cards out of the sleeve AND use the cards for transactions that have nothing to do with crossing the border. The "unique ID number" on the RFID chip can be easily collected, along with other personal information from a transaction – such as name and address from the driver's license, or a credit card number. Therefore, the "unique ID number" will cease to be an anonymous, meaningless number as DHS and the State Department assert. Once a person's identity is associated with the RFID chip, he or she can be unknowingly identified or tracked by a network of compatible readers.

Also, because the RFID chip includes information about the issuing entity, Americans traveling abroad could be identified as such and be vulnerable to security risks.

Lastly, because the "unique ID number" on the RFID chip is transmitted in the clear, unscrupulous individuals might be able to use the number to access personal information held in government databases. Recent privacy breaches at the State Department support this concern.

Finally: I would like to offer some recommendations.

(1) This Subcommittee should press DHS and the State Department to abandon vicinity RFID technology in favor a machine-readable technology that requires the card to make contact with the reader. This is consistent with the Departments' goal of "pre-positioning" traveler information.

(2) In addition, this Subcommittee should insist that the citizen's unique ID number be encrypted or otherwise protected from unauthorized readers. This how the new electronic passport works.

(3) This Subcommittee should also strongly consider supporting legislation or regulations that prohibit the unauthorized skimming of the RFID chip by businesses and other third parties.

(4) Finally, this Subcommittee should consider supporting legislation or regulations that prohibit the use of the passport card and Enhanced Driver's License by government agencies that have nothing to do with border security.

I welcome any questions the Subcommittee might have.