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

January 23, 2007

Office of Passport Policy, Planning & Advisory Services
Bureau of Consular Affairs
U.S. Department of State
2100 Pennsylvania Ave. NW, Suite 300
Washington, DC 20037

Re: **Additional comments on** *Card Format Passport; Changes to Passport Fee Schedule*
Docket ID: DOS-2006-0393
22 CFR Parts 22 and 51
RIN 1400-AC22
[Public Notice 5558]

Dear Sir or Madam:

On January 7, we submitted comments on the passport (or PASS) card proposed rule, including the decision to add a "vicinity read" RFID tag to the card. After we submitted our comments, we received feedback that we believe is important. While we understand that the official comment period is closed, we strongly urge the Departments of State and Homeland Security to investigate and clarify the RFID tag password issue.

In our section entitled "Tag Password is Discoverable," we asserted that the GEN-2 protocol calls for a 32-bit password that controls access to the Electronic Product Code (EPC). We argued, however, that the password is discoverable by power analysis attack or eavesdropping, thereby putting the Unique Reference Number at risk of being uncovered – and thus creating a significant privacy risk for the PASS Card holder. After we submitted our comments to the State Department, we were informed that although an earlier iteration of the GEN-2 protocol did provide for a password to control access to the EPC, the current version of the protocol (1.0.9) does *not* include an access password protecting the EPC. Rather, the 32-bit access password protects *other memory* on the GEN-2 RFID tag.

This is a nuanced technical point that is not clear in the literature we have read, but we believe it is an important one. We highlighted privacy concerns assuming the password controlled access to the URN. If in fact there is no way to password-protect the URN, then our privacy arguments are even more salient. We strongly urge the Departments of State and Homeland Security to clarify: Does the GEN-2 RFID technology chosen for the PASS Card allow for the URN to be password protected, and what are the privacy implications of the answer to that question?

Sincerely,

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