DEPARTMENT OF STATE

Docket No. DOS-2006-0329
Proposed Rule: Card Format Passport; Changes to Passport Fee Schedule

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on October 17, 2006, the Department of State ("DOS") seeks to create the People Access Security Service ("PASS") card, which would be used for "international land and sea travel between the U.S., Canada, Mexico, the Caribbean, and Bermuda."[1] Pursuant to this DOS notice, the Electronic Privacy Information Center ("EPIC") submits these comments to request that DOS reject the use of "vicinity read" radio frequency identification technology in the Western Hemisphere Travel Initiative PASS card, because it contains substantial privacy and security risks, such as "skimming" and "eavesdropping"; it does not contain Basic Access Control; and the cost of its creation is prohibitive. In the alternative, if the Department of State does choose to create the PASS card, we urge the agency to delay implementation until the current problems, explained below, are solved.

Introduction

EPIC has submitted a series of comments on proposals undertaken by federal entities regarding the use of radio frequency identification ("RFID") technology.[2] In April 2005, we joined other civil liberties and technology groups in submitting comments urging the Department of State to abandon its proposal, because it would have made

[1] Department of State, *Card Format Passport; Changes to Passport Fee Schedule Proposed Rule*, 71 Fed. Reg. 60928 (Oct. 17, 2006) *available at* http://www.epic.org/privacy/surveillance/spotlight/0806/pass_fr.html.
[2] *See generally* EPIC's page on Radio Frequency Identification (RFID) Systems, http://www.epic.org/privacy/rfid/.

personal data contained in hi-tech passports vulnerable to unauthorized access.[3] In August and October 2005, we urged the Department of Homeland Security to abandon the use RFID technology in its I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program; or, in the alternative, to delay such use until the findings of ongoing RFID testing are released and current privacy and security risks are eliminated.[4] And in December 2005, we again explained the problems with the use of RFID in the E-passport and I-94 forms in comments to the Department of Homeland Security Data Privacy and Integrity Advisory Committee.[5] Now, we write to urge the Department of State to reconsider this proposal to use "vicinity" RFID technology in the Western Hemisphere Travel Initiative PASS Card.[6]

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[7] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection,

[3] EPIC, EFF et. al, Comments on RIN 1400-AB93: Electronic Passport (Apr. 4, 2005) *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.
[4] EPIC, Comments on Docket No. DHS-2005-0040: Notice of Privacy Act System of Records: The Automated Identification Management System (Aug. 4, 2005) *available at* http://www.epic.org/privacy/us-visit/comments080405.pdf; EPIC, Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry (Oct. 3, 2005) *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.
[5] EPIC, Comments on Docket No. DHS-2005-0047: Notice of Public Meeting and Request for Comments (Dec. 6, 2005) *available at* http://www.epic.org/privacy/us-visit/comm120605.pdf.
[6] EPIC also discussed the PASS Card in a Spotlight on Surveillance report, *Homeland Security PASS Card: Leave Home Without It* (August 2006), http://www.epic.org/privacy/surveillance/spotlight/0806/.
[7] S. Rep. No. 93-1183 at 1 (1974).

> maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[8]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[9] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[10] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[11] Adherence to these requirements is critical for a system such as the PASS Card, which would be required for millions of American citizens and lawful permanent residents who travel to Canada and Mexico by land and to the Caribbean and Bermuda by sea.[12]

The Intelligence Reform and Terrorism Prevention Act of 2004 mandated that, by January 2008, the departments of Homeland Security and State develop and implement a plan to require U.S. citizens and foreign nationals to present a passport or other documents to prove identity and citizenship when entering the United States from certain

---

[8] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[9] S. Rep. No. 93-1183 at 1.
[10] Pub. L. No. 93-579 (1974).
[11] *Id*.
[12] Press Release, Department of State, *Department of State to Introduce Passport Card* (Oct. 17, 2006).

countries in North, Central or South America.[13] This program is called the Western Hemisphere Travel Initiative, and its impact is the greatest upon U.S. citizens who routinely cross the border. Accepted documents for U.S. citizens will be either a valid U.S. passport or the proposed PASS card.[14] This is a significant change from the previous system, where U.S. citizens would show a driver's license, birth certificate or nothing at all to cross the border. Approximately 23 million U.S. citizens cross the border to Mexico or Canada about 130 million times per year.[15]

I. DOS Should Abandon Use of "Vicinity" RFID Technology in the PASS Card Because of Substantial Privacy and Security Threats

Under the Western Hemisphere Travel Initiative, U.S. citizens would have to carry either a passport or a PASS card. There are significant privacy and security risks associated with the use of RFID-enabled PASS cards to track the entry and exit of U.S. citizens, particularly if individuals are not able to control the disclosure of identifying information. They include the risks of "skimming," and "eavesdropping." These risks are enhanced with the use of "vicinity" or "long-range" RFID tags.

Last month, the Department of Homeland Security Data Privacy and Integrity Advisory Committee ("DPIAC") adopted a report, "The Use of RFID for Identity Verification," which included recommendations concerning the use of RFID in

[13] Pub. L. No. 108-408, §7209, 118 Stat. 3638, 3823 (2004).
[14] 71 Fed. Reg. at 60928.
[15] Frank Moss, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, Department of State, *Hearing on Proposed Western Hemisphere Passport Rules: Impact on Trade and Tourism Before the Subcom. on Immigration, Border Security and Citizenship of the S. Judiciary Comm.*, 108th Cong. (Dec. 2, 2005) *available at* http://judiciary.senate.gov/testimony.cfm?id=1714&wit_id=4868.

identification documents.[16] The committee outlined security and privacy threats associated with RFID similar to the ones discussed above, and it urged against using RFID technology unless the technology is the "least intrusive means to achieving departmental objectives. The long-range RFID-enabled PASS card is not the least-intrusive means, as that would be for an individual to hand the PASS card to a border control official. The proposed technical standard for the PASS card thus fails to comply with the DHS Data Privacy and Integrity Advisory Committee's recommendations regarding the use of RFID technology.

The data on the PASS card would include the personal information currently displayed in passports, "bearer's facial image, full name, date and place of birth, passport card number, dates of validity and issuing authority," and the reverse side would include "a machine-readable zone."[17] The card "will use a full facial image printed on the card as the biometric identifier."[18] The PASS card also will "utilize Radio Frequency (RF) technology to store and transmit" a unique reference number to the border official so that she may access the traveler's information in a large federal database, "which could include additional information, for example, information about the bearer's membership in one of [Customs and Border Protection's] international trusted traveler programs."[19]

Although DOS states that the RFID tags will only carry a unique reference number, which will not contain any personally identifiable information, the numbers are linked to data files, and are subject to interception. The reference number is the key that

[16] Department of Homeland Security, Data Privacy and Integrity Advisory Committee, *The Use of RFID for Human Identity Verification (Report No. 2006-02)* (Dec. 6, 2006) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.
[17] 71 Fed. Reg. at 60930.
[18] *Id*.
[19] *Id*.

permits access to records in the federal database.[20] Anytime a U.S. citizen is carrying his RFID-enabled PASS card, his unique reference number, which is linked to his individual biographic information, could be accessed by unauthorized individuals. And because the RFID wireless technology is unseen, the person would not know that his information was intercepted. In many respects, the unique "reference number" issued by the Department of State for the PASS card could operate like the Social Security Number, linking together discrete databases and creating many of the same privacy risks that have arisen with the Social Security Number.

Privacy and security risks associated with RFID-enabled identification cards include "skimming" and "eavesdropping." Skimming occurs when an individual with unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader. The Government Accountability Office has said that "without effective security controls, data on the tag can be ready by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users."[21]

The RFID chip embedded in the PASS card would be passive (without an internal power source), and it would utilize, "vicinity read technology" that "would allow the

[20] "This reference number will be assigned by Department of State at the time the passport card is issued." *Id*.
[21] Gregory C. Wilshusen, Director Information Security Issues, Government Accountability Office, *Hearing on Ensuring the Security of America's Borders through the Use of Biometric Passports and Other Identity Documents Before the Subcom. on Economic Security, Infrastructure Protection, and Cybersecurity of the H. Comm. on Homeland Security*, 108th Cong. (June 22, 2005*) available at* http://www.gao.gov/cgi-bin/getrpt?GAO-05-849T.

passport card data to be read at a distance of up to 20 feet from the reader."[22] This is a long distance, much longer than the few inches that would be necessary to hand a PASS card to a border official. This longer distance increases the security risk, as unauthorized readers could be hidden a significant distance from the PASS cardholder. For example, in the border-crossing scenario where many people are gathered together, it is conceivable that an attacker could carry a concealed RFID-reader that would enable the capture of the "unique reference number" for the PASS card from those in close proximity. This risk would be avoided if the Department of State would continue to use paper documents or would rely upon machine-readable documents that require contact with the reader device for identification.

As the PASS cards, like U.S. passports, will be valid for 10 years, it is certain that new means of attack will be developed.[23] Though the creation of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches.[24] But, DOS is proposing "vicinity read" RFID technology, where the tags can be read at 20 feet or more. In the RFID-enabled I-94 forms, the Department of Homeland Security states, "reliable reads can be received from a few inches to as much as 30 feet away from the reader."[25] And other tests also have shown that RFID tags can be read

---

[22] 71 Fed. Reg. at 60931.
[23] "[P]assport cards, like passport books, would be issued for a ten-year validity period for U.S. citizens sixteen years old and older, and for a five-year validity period for U.S. citizens less than 16 years of age." *Id*. at 60930.
[24] *See generally* Wikipedia entry on Radio Frequency Identification, http://en.wikipedia.org/wiki/Rfid.
[25] Department of Homeland Security, *Notice with request for comments*, 70 Fed. Reg. 44934, 44395 (Aug. 5, 2005) *available at* http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve.

from 70 feet or more, posing a significant risk of unauthorized access.[26] Some attacks already have succeeded so-called "strengthened" identification documents. In one case, a computer expert was able to clone the United Kingdom's electronic passport by using a commercially available RFID reader (which cost less than $350) and software that took him less than a couple of days to write.[27] In assessing the new RFID-enabled U.S. passports, one expert cloned the RFID tag and another used characteristics of the radio transmissions to identify individual chips, and, as security expert Bruce Schneier has pointed out, the researchers spent only a few weeks attacking the RFID-enabled passport.[28] Criminals would have 10 years to attack the PASS card, if it is created as proposed. The aforementioned security and privacy threats are reasons why DOS should abandon the use of any RFID technology, especially long-range or "vicinity", in the PASS card.

II. The Proposed RFID-enabled PASS Card Lacks Basic Access Control

The "vicinity" RFID-tagged PASS Cards would allow the automatic identification and documentation of the entry and exit of covered individuals. By design, this system will enable the surreptitious monitoring of individuals and, specifically, the capture of identifying information without the individual's knowledge or consent.

In the absence of effective security techniques, RFID tags are remotely and secretly readable. Security expert Bruce Schneier has noted, "Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot of this is that

---

[26] *See* Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, Feb. 22, 2005 *available at* http://eprint.iacr.org/2005/052; Scott Bradner, *An RFID warning shot*, Network World, Feb. 7, 2005.
[27] Steve Boggan, *Special Report: Identity Cards: Cracked It!*, Guardian, Nov. 17, 2006.
[28] Bruce Schneier, Opinion, *The ID Chip You Don't Want in Your Passport*, Wash. Post, Sept. 16, 2006.

travelers carrying around RFID passports are broadcasting their identity."[29] This demonstrates another security risk of the long-range RFID-enabled PASS card proposal, that of clandestine tracking. An unauthorized RFID reader could be constructed to mimic the authorized signal and then be used to secretly read the RFID tag embedded in the PASS cards.

The Government Accountability Office has highlighted this security problem unique to wireless technology:

> The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated.[30]

Anytime a visitor is carrying his long-range RFID-tagged PASS card, his unique identification number, which is linked to his individual biographic information, could be accessed by unauthorized individuals. So long as the RFID tag or chip can be read by unauthorized individuals, the person carrying that tag can be distinguished from any other person carrying a different tag. Foreign visitors could be identified as such merely because they carry an RFID-enabled PASS card.

The Department of State proposes to issue a "thin protective sleeve, which is designed to protect the card from unauthorized access. The card could be stored in the sleeve and removed only when needed."[31] This is a good security feature, but it is an acknowledgment by DOS that there is a threat of unauthorized access to the RFID tag

---

[29] Bruce Schneier, Opinion, *Passport radio chips send too many signals*, Int'l Herald Tribune, Oct. 4, 2004.
[30] Government Accountability Office, *Report to Congressional Requesters: Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (May 2005) *available at* http://www.gao.gov/new.items/d05551.pdf.
[31] 71 Fed. Reg. at 60931.

embedded in the PASS cards.

This approach is contrary to the recommendation of the International Civil Aviation Organization ("ICAO"). ICAO had earlier proposed that strong security features be implemented in all machine-readable travel documents.[32] Specifically, ICAO recommends incorporation of Basic Access Control in identification documents. ICAO explains, "[a] chip that is protected by the Basic Access Control mechanism denies access to it's [sic] contents unless the inspection system can prove that it is authorized to access the chip."[33]

The authorization needed could be a secret key or password used to unlock the data. To obtain the key, the border officer would need to physically scan the machine-readable text that is printed on the RFID-enabled PASS card. The RFID tag reader would then hash the data to create a unique key that could be used to authenticate the reader and unlock the data on the RFID chip. Basic Access Control prevents skimming by preventing remote readers from accessing the data on the document. The data cannot be read unless the document is physically opened and scanned through a reader. It also prevents eavesdropping by encrypting the communication channel that opens when data is sent from the chip to the RFID reader. The Basic Access Control solution does not, however, solve all security and privacy concerns.

DOS should be fully aware by now of the problems raised by an RFID scheme lacking Basic Access Control. After DOS received more than 2,400 comments on its notice for proposed rulemaking on RFID-enabled passports, many of which criticized its

[32] ICAO, Machine Readable Travel Documents, *Technical Report: PKI for Machine Readable Travel Documents Offering ICC Read-Only Access*, version 1.1 (Oct. 1, 2004) *available at* http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf.
[33] *Id*. at 16.

serious disregard of security and privacy safeguards, the agency said it would implement Basic Access Control that would prevent skimming and eavesdropping.[34] The RFID implementation proposed in the PASS card contravenes the Department of State's incorporation of basic security features into new U.S. passports.[35]

The principle of Basic Access Control is critical to the design of identification systems. Individuals, unlike commercial products with RFID tags, should have the right to control the disclosure of their identifying information. If the Department of State does implement the long-range RFID-enabled PASS card proposal, it should at least incorporate Basic Access Control or equivalent security features, into the cards.

III. Cost of PASS Card to Individuals and the United States Is Prohibitive

Though the price of the PASS card itself would not be prohibitive, there are other costs to consider.[36] These include costs to the United States and its citizens in international trade and stemming from creation of an infrastructure for the long-range RFID-enabled PASS card.

There are costs for the reader equipment. In May, the Government Accountability Office found that a problem associated with the PASS card is that "no all land ports of entry currently have equipment to read documents, and existing equipment may not be compatible with the approach chosen."[37]

---

[34] Notice of Proposed Rule, 70 Fed. Reg. 8305 (Feb. 18, 2005) *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.
[35] *See* Kim Zetter, *Feds Rethinking RFID Passport*, Wired, Apr. 26, 2005; Eric Lipton, *Bowing to Critics, U.S. to Alter Design of Electronic Passports*, New York Times, Apr. 27, 2005.
[36] The PASS card would cost $20 for those ages 16 and up and $10 for those under age 16, and applicants might also have to pay a $25 "execution fee." 71 Fed. Reg. at 60931.
[37] Government Accountability Office, *Observations on Efforts to Implement the Western Hemisphere Travel Initiative on the U.S. Border with Canada,* GAO-06741R (May 25, 2006) *available at* http://www.gao.gov/new.items/d06741r.pdf.

There is also the cost to U.S. citizens in terms of international trade. For example, Sen. Patrick Leahy said that his state of Vermont would be significantly affected. In 2004, "Vermont exported $1.516 billion worth of products to Canada.... Policies that hamper this trade have obvious and serious consequences for Vermont businesses and workers."[38] There are concerns about the effect on the U.S. tourism industry. "In 2003, more than two million Canadians visited Vermont and spent $188 million while here. If these new burdens discourage Canadians and other foreign visitors from traveling to Vermont, our tourism industry will feel it," Sen. Leahy said.[39] And Vermont is just one of the many border states that would be affected.

Conclusion

The Department of Homeland Security and associated federal agencies have been increasingly proposing RFID technology in its identification documents. As the proposed Western Hemisphere Travel Initiative PASS card, U.S. passport, and US-VISIT I-94 entry and exit forms all contain RFID chips, if the PASS card proposal is adopted, then all U.S. citizens carrying either a passport or PASS card and visitors entering the country through US-VISIT will be able to be tracked using RFID technology.

In a speech last month, Homeland Security Secretary Michael Chertoff said he "welcome[d] increased oversight, because I welcome debate about the fundamental strategy that we are undertaking in homeland security. This is a set of decisions the American people, in their entirety, must own because we will all live with the

[38] Statement of Senator Patrick Leahy, *Hearing on Proposed Western Hemisphere Passport Rules: Impact on Trade and Tourism Before the Subcom. on Immigration, Border Security and Citizenship of the S. Judiciary Comm.*, 108th Cong. (Dec. 2, 2005) *available at* http://judiciary.senate.gov/member_statement.cfm?id=1714&wit_id=2629.
[39] *Id*.

consequences of these choices."[40] Because we will all have to live with the consequences of using the proposed long-range RFID-enabled PASS card, and because of the privacy and security risks associated with the card, we urge against its creation. We urge the Department of State to abandon the use of RFID technology in the PASS card; or, in the alternative, to delay such use until current privacy and security risks are adequately assessed.

Respectfully submitted,

Marc Rotenberg
Executive Director

Melissa Ngo
Director, Identification and
Surveillance Project

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

[40] Department of Homeland Security, *Remarks by Homeland Security Secretary Michael Chertoff on Protecting the Homeland Security: Meeting Challenges and Looking Forward* (Dec. 14, 2006) *available at* http://www.dhs.gov/xnews/speeches/sp_1166137816540.shtm.