DEPARTMENT OF HOMELAND SECURITY

Data Privacy and Integrity Advisory Committee
Docket No. DHS-2005-0047
Notice of Public Meeting and Request for Comments

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on November 16, 2005, the Department of Homeland Security Data Privacy and Integrity Advisory Committee ("DPIAC") requested public comments and announced a public meeting.[1] Pursuant to this DPIAC notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the use of radio frequency identification (RFID) tags in the United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program and the E-Passport program.

According to documents very recently obtained by EPIC under the Freedom of Information Act, government testing of the RFID-enabled passports uncovered many problems with the program.[2] Tests conducted last year by the Department of Homeland Security revealed, among various problems, that "contactless" RFID technology does not improve the efficiency of the inspection process, but rather distracts inspectors from their duties.[3] Due to this failure and the significant privacy and security risks involved in the use of RFID technology, EPIC urges the Department of Homeland Security to abandon

---

[1] Notice of Federal Advisory Committee Meeting, 70 Fed. Reg. 69583 (Nov. 16, 2005).
[2] Department of Homeland Security, International Civil Aviation Organization, and International Organization for Standardization, *E-Passport Mock Port of Entry Test November 29 thru December 2, 2004: Operational Impact on the Inspection Process* obtained by EPIC through FOIA requests (hereinafter "EPIC RFID FOIA") *available at* http://www.epic.org/privacy/us-visit/foia/mockpoe_res.pdf.
[3] *Id*.

the use of "contactless" RFID technology in the E-Passport and to review carefully all the applications that may require the use of RFID technology in identification documents, including the I-94 and I-94W forms.

Introduction

EPIC has submitted a series of comments on database proposals undertaken regarding the development of the US-VISIT program and the E-Passport. In February 2004, EPIC first wrote to urge DHS to determine how it will apply Privacy Act obligations to the US-VISIT program, to consider the significance of international privacy standards in the collection and use of personal information by the agency on non-U.S. citizens, and to prohibit the expansion of US-VISIT uses outside the program's defined mission.[4] Next, we warned DHS that, in its continued implementation of US-VISIT, it must further protect against the dangers of mission creep, evaluate the accuracy and security of its pilot program, and recognize a right of judicial review for individuals adversely affected by the program.[5] As we did in August[6] and October 2005,[7] EPIC now urges that the Department of Homeland Security reject this proposal to incorporate a "contactless" RFID tag into the form I-94 and I-94W.

In April 2005, EPIC, the Electronic Frontier Foundation, and other groups submitted comments urging the State Department to abandon its E-Passport proposal, because it would have made personal data contained in hi-tech passports vulnerable to

[4] Comments of the Electronic Privacy Information Center, Docket No. BTS 03-01 (Feb. 4, 2004) *available at* http://www.epic.org/privacy/us-visit/us-visit_comments.pdf.
[5] Comments of the Electronic Privacy Information Center, Docket No. DHS-2007-0002 (Nov. 5, 2004) *available at* http://www.epic.org/privacy/us-visit/us-visit_comments2.pdf.
[6] Comments of the Electronic Privacy Information Center, Docket No. DHS-2005-0040 (Aug. 4, 2005) *available at* http://www.epic.org/privacy/us-visit/comments080405.pdf.
[7] Comments of the Electronic Privacy Information Center, Docket No. DHS-2005-0011 (Oct. 3, 2005) *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

unauthorized access.[8] The State Department reevaluated the E-Passport plan after receiving a storm of criticism, but the proposal is going forward.[9]

I. DHS Should Abandon the Use of RFID Technology in the E-Passport Because Previous Tests Show Its Failures

The United States is moving aggressively to implement a new electronic passport ("E-Passport"). By October 2006, almost all U.S. passports will include an RFID-enabled chip containing about a unique identification number for the passport holder.[10] The E-Passport program is being implemented "as soon as possible," according to the State Department, "[i]n order to protect the security of U.S. borders."[11]

EPIC, the Electronic Frontier Foundation, and other groups submitted comments urging the State Department to abandon its E-Passport proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access.[12] Proponents claimed that E-Passports would improve the inspection process at the borders, but documents obtained last week by EPIC under Freedom of Information Act reveal wide-ranging problems with the program.

The EPIC FOIA documents show that tests conducted last year by the Department

---

[8] EPIC, EFF et. al, Comments on RIN 1400-AB93: Electronic Passport (Apr. 4, 2005) (hereinafter "EPIC E-Passport Comments") *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.

[9] Of the 2,335 comments received by the State Department about its Electronic Passport proposal, 98.5% were negative comments, Notice of Final Rule, 70 Fed. Reg. 61553 (Oct. 25, 2005) (hereinafter "E-Passport Notice"); Comments submitted to the State Department regarding its Electronic Passport proposal *available at* http://travel.state.gov/passport/eppt/passport_comments.php.

[10] *Id*.; Leslie Miller, *New Passports Will Have High-Tech Features,* Associated Press, Oct. 25, 2005; Jonathan Krim, *U.S. Passports to Receive Electronic Identification Chips*, Washington Post, Oct. 26, 2005.

[11] E-Passport Notice at 61555, *supra* note 9.

[12] EPIC E-Passport Comments, *supra* note 8.

of Homeland Security on sample "E-Passport readers" found problems associated with the use of RFID. Among them: "Insufficient power to read all variations of chips on many readers," "Most units required knowledge of where chip was in order to perform accurate read, required substantial manipulation of the passport," "Footprint of the units interferes with inspector operations," and "Some readers required the inspector to hold the passport firmly against the unit in order to perform the read. This means the inspector is not able to perform other parts of the inspection" (emphases in original).[13]

According to the Department of Homeland Security, "[i]nspectors must keep their eyes on the traveler at all times," yet the E-Passports take the inspectors' attention away from travelers.[14] According to the EPIC FOIA documents, the DHS tests found that "[i]nstructions on the reader distract the inspector, e.g. electronic displays," and "[r]eaders require too much attention and time on the part of the inspector."[15] The use RFID technology is detrimental to the security and efficiency goals of the inspection process, and EPIC urges the Department of Homeland Security and the State Department to abandon the E-Passport proposal.

II. DHS Should Abandon the Use of RFID Technology in the I-94 and I-94W Forms Because of Security and Privacy Threats

In an August 2005 notice, US-VISIT announced that RFID tags will be embedded in the Form I-94 or Form I-94W, which is the Arrival-Departure record issued to a traveler to the United States.[16] Individuals subject to US-VISIT are required to provide fingerscans, photographs, or other biometric identifiers upon arrival in, or departure from,

[13] EPIC RFID FOIA at 10, 11, *supra* note 2.
[14] *Id*. at 18.
[15] *Id*. at 11.
[16] Notice with request for comments, 70 Fed. Reg. 44934 (Aug. 5, 2005) (hereinafter "Aug. 2005 Notice").

the United States. This test program, which began on August 31, 2005 and will last one year, will "automatically document[] the exits and any subsequent re-entries of nonimmigrant travelers at five United States land border ports-of-entry crossings utilizing radio frequency identification (RFID) technology."[17] According to the agency, "[t]he purpose of this testing is to determine if RFID technology can improve the efficiency of processing individuals who seek to enter or exit the United States at a land border port-of-entry."[18]

The agency further stated that, "The purpose of an RFID system is to enable data to be transmitted by a portable device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information."[19] Under US-VISIT, all aliens are subject to biometric collection, biographic data collection, and watch list checks. The information collected from individuals includes name, date of birth, gender, country of citizenship, passport number and country of issuance, complete U.S. destination address, arrival and departure information, a digital photograph, and digital fingerscans.[20]

According to the August 2005 notice, the RFID tag will be embedded in I-94 and I-94W forms:

> The tag will be powered by the radio frequencies transmitted by transceivers that will be mounted at both vehicular and pedestrian exit lanes at select land border ports-of-entry… DHS will be able to automatically identify and document the exits and, if applicable, the subsequent re-entry of select travelers at the United States land border ports-of-entry identified in the proof of concept protocol.[21]

---

[17] *Id.*
[18] *Id*.
[19] EPIC's Radio Frequency Identification (RFID) Systems page, *available at* http://www.epic.org/privacy/rfid/.
[20] Notice of Availability of Privacy Impact Assessment, 70 Fed. Reg 39300, 39305 (July 7, 2005).
[21] Aug. 2005 Notice at 44396, *supra* note 16.

The use of RFID tags in I-94 forms creates significant security and privacy risks, particularly if individuals are not able to control the disclosure of identifying information. By their very design 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 travelers carrying around RFID passports are broadcasting their identity."[22] This demonstrates a security risk of the RFID-enabled I-94 form proposal, that of clandestine tracking. DHS claims that, "[i]t will not be possible to track the whereabouts of a person in the United States because DHS is using non-battery powered passive tags. The tags themselves can only be activated by the radio wave sensors used at one of the proof of concept land ports-of-entry and within the port of entry."[23] This is untrue. An unauthorized RFID reader could be constructed to mimic the authorized US-VISIT signal and then be used to secretly read the RFID tag embedded in the I-94 and I-94W forms.

Anytime a visitor is carrying his I-94 RFID-enabled form, 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 I-94 form. Individuals would not be able to control the disclosure of their information.

---

[22] Bruce Schneier, Opinion, *Passport radio chips send too many signals*, Int'l Herald Tribune, Oct. 4, 2004.
[23] Aug. 2005 Notice at 44397, *supra* note 16.

Problems in the RFID-enabled I-94 form proposal are similar to the ones created by the initial State Department E-Passport proposal about which EPIC and others submitted comments. These problems include skimming and eavesdropping. Skimming occurs when information from an RFID chip is surreptitiously gathered by an unauthorized individual. Eavesdropping occurs when an individual intercepts data as it is read by an authorized RFID reader. Tests have shown, and DHS admits, that RFID tags can be read from thirty feet or more, posing a significant risk of unauthorized access.[24]

Conclusion

RFID is an invisible technology with security and privacy implications. It allows a person's information to be accessed without his or her knowledge. Government testing of E-Passport readers conducted just last year shows that use of the technology at ports-of-entry impedes the inspection process. Because of this failure and the significant privacy and security risks associated with the technology, EPIC urges the Department of Homeland Security to abandon the use of RFID technology in E-Passports and in the US-VISIT program.

Respectfully submitted,

_____

Marc Rotenberg
Executive Director

[24] DHS states that, with these tags, "reliable reads can be received from a few inches to as much as 30 feet away from the reader," Aug. 2005 Notice at 44395, *supra* note 16; *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 *available at* http://www.networkworld.com/columnists/2005/020705bradner.html.

Cédric Laurant
Director, International Privacy Project

Melissa Ngo
Staff Counsel