DEPARTMENT OF HOMELAND SECURITY
Privacy Office

Docket No. DHS-2005-0040
Notice of Privacy Act System of Records
The Automated Identification Management System

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

On July 5, 2005, the Department of Homeland Security ("DHS") published notice that it proposed to add a system of records, the Automated Identification Management System ("AIDMS"), to its inventory of record systems. The AIDMS will be "used to facilitate and further automate processes for entry into and exit from the United States through the issuance to covered individuals, of a radio frequency identification tag with a unique identifier."[1] According to the notice, these 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. The AIDMS is part of an effort to expand the United States Visitor and Immigrant Status Indicator Technology program ("US-VISIT"). Individuals subject to US-VISIT are required to provide fingerscans, photographs, or other biometric identifiers upon arrival in, or departure from, the United States. US-VISIT has been implemented in "increments." As part of "Increment 2," US-VISIT will test the use of passive RFID tags to "automatically, passively, and remotely" record the entry and exit of covered individuals.[2]

Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the program's proposal to use RFID-enabled I-94 forms to track the entry and exit of visitors. EPIC urges the Department of Homeland Security to abandon the use of "contactless" RFID technology in its I-94 forms; or,

[1] Notice of Privacy Act systems of records, 70 Fed. Reg. 38699 (July 5, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13215.htm.
[2] *Id.*

in the alternative, to delay such use until the findings of ongoing RFID testing are released and current privacy and security risks are eliminated. EPIC also opposes the proposed routine use exceptions that would clearly contravene the narrow purpose of automating the "processes for entry into and exit from the United States."

Introduction

EPIC has submitted a series of comments on database proposals undertaken by the DHS regarding the development of the US-VISIT program. First, we wrote to urge DHS to determine how it will apply Privacy Act obligations to the 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.[3] 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.[4] Now, we write to urge the Department to reconsider this proposal to incorporate a "contactless" RFID tag in the form I-94.

I. DHS Should Abandon the Use of RFID Technology in US-VISIT Because of Security and Privacy Threats

The US-VISIT program is testing the use of RFID technology for its data files. "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.

[3] 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.
[4] 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.

The data transmitted by the tag may provide identification or location information."[5] 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.[6]

According to the Privacy Act notice, "[t]he RFID tag, which will contain a unique identification code, will be linked at a POE [point of entry] with the biographic and biometric information that was collected when the traveler entered the United States." The notice goes on to describe a seemingly narrow application for the RFID tag:

> When travelers either drive or walk through the port-of-entry, a transceiver will send out a harmless radio wave frequency that will power the DHS-issued RFID tag to transmit back a unique identifier code number. This code number, when received by the transceiver, will be relayed back to secure DHS computer systems and matched with the biographic and/or biometric data of the traveler. The RFID tag number will not contain or be derived from any personal information. DHS will be able to automatically identify and document the exits and, if applicable, the subsequent re-entry of covered individuals.[7]

DHS is aware that the use of RFID tags in this context raises security and privacy concerns. DHS states that after conducting an operational alternatives assessment, passive RFID technology was determined to best satisfy the program's needs.[8] DHS said passive RFID tags would: (1) protect personal privacy by controlling the use of personal information outside of DHS systems; (2) minimize the surreptitious tracking of travelers outside the port of entry because it does not constantly transmit a signal; and (3) protect personal privacy by reading only

[5] EPIC's Radio Frequency Identification (RFID) Systems page, *available at* http://www.epic.org/privacy/rfid/.
[6] Notice of Availability of Privacy Impact Assessment, 70 Fed. Reg 39300, 39305 (July 7, 2005) *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm.
[7] 70 Fed. Reg. at 38699, 38700.
[8] *Id.* at 39310.

a unique number from an embedded chip in a new Form I-94.[9] However, the use of passive or active 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.

Although DHS states that the RFID tags will only carry a unique identification number, which will not contain any personally identifiable information, the ID numbers are linked to data files, and are subject to interception.[10] The ID number is the key that permits access to records in the US-VISIT system. As the Privacy Act notice states, "Information may be searched and retrieved based on various data elements, including, but not limited to: RFID tag number, traveler identification number, transaction number, and name of covered individual."[11]

By their very design RFID tags, whether passive or active, are remotely and secretly readable. Security expert Bruce Schneier 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."[12] This demonstrates another security risk of the RFID-enabled I-94 form proposal, that of clandestine tracking. DHS claims, "that the unencrypted RFID tag number will not be structured in such a way that it can be used to identify the individual as a non-immigrant,"[13] This is untrue. DHS itself said in July 7, 2005 revised Privacy Impact Assessment that there is a risk that the RFID tag "could be used to conduct surreptitious locational surveillance of an individual; i.e., to use the presence of the tag to follow an individual as he or she moves about in the U.S."[14]

---

[9] *Id*. Passive tags "carry no on-board source of power, and instead derive power indirectly from the interrogating signal of a reader," while active tags are self-powered.
[10] *Id*.
[11] *Id*. at 38701.
[12] Bruce Schneier, Opinion, *Passport radio chips send too many signals*, Int'l Herald Tribune, Oct. 4, 2004.
[13] 70 Fed. Reg. at 39310.
[14] *Id.*

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.

The problems with the proposal to use RFID-enabled I-94 forms are very similar to the problems found in the State Department's flawed proposal to include RFID tags in U.S. passports. The State Department is reassessing the plan after receiving a storm of criticism. EPIC, the Electronic Frontier Foundation, and other groups, submitted comments urging the State Department to abandon its proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access.[15] Problems in the passport proposal, which are also problems in the RFID-enabled I-94 form proposal, 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 that RFID tags can be read from thirty feet or more, posing a significant risk of unauthorized access.[16]

RFID is an invisible technology. It allows a person's information to be accessed without his or her knowledge. The slight time-saving benefits of RFID-enabled I-94 forms are heavily outweighed by the significant privacy and security risks. In light of this, EPIC urges DHS to

[15] 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.
[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.

abandon the use of RFID in the US-VISIT program. In the alternative, DHS should continue to assess the RFID I-94 card and not implement it in the US-VISIT program until further results of testing are completed and the security and privacy risks can be eliminated.

II. The Proposed RFID Implementation Lacks Basic Access Controls

According to the Federal Register notice, the Department intends to test passive RFID tags that will "*automatically, passively, and remotely*" record the entry and exit of covered individuals (emphasis added).[17] 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.

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.[18] Specifically, ICAO recommends incorporation of Basic Access Control ("BAC") 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."[19]

The authorization needed could be a secret key or password used to unlock the data. To obtain the key, the Customs officer would need to physically scan the machine-readable text that is printed on the RFID-enabled I-94 form. 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. BAC prevents skimming by preventing remote readers from accessing the data on the

[17] 70 Fed. Reg. at 38699.
[18] 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.
[19] *Id*. at 16.

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 BAC solution does not, however, solve all security and privacy concerns.

The DHS should be fully aware by now of the problems with an RFID scheme that lacks BAC. After the State Department received more than 2,400 comments on its notice for proposed rulemaking on RFID passports,[20] many of which criticized its serious disregard of security and privacy safeguards, the agency said it would implement a BAC that would prevent skimming and eavesdropping, The RFID implementation proposed by DHS contravenes representations made by the U.S. State Department regarding the incorporation of basic security features into new U.S. passports. [21]

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 Homeland Security does implement the RFID proposal, it should at least incorporate Basic Access Control or equivalent security features, into the RFID-enabled I-94 forms.

III. DHS Should Not Permit Routine Uses for an RFID Application that is Simply Intended to Automate the "processes for entry into and exit from the United States"

The public notice about the AIDMS system of records states that, in addition to those disclosures permitted under the Privacy Act, the "routine uses" of the information would be

[20] 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.
[21] *See* Kim Zetter, "*Feds Rethinking RFID Passport*," Wired, Apr. 26, 2005, *available at* http://www.wired.com/news/privacy/0,1848,67333-2,00.html?tw=wn_story_page_next1; Eric Lipton, "*Bowing to Critics, U.S. to Alter Design of Electronic Passports*," New York Times, Apr. 27, 2005, *available at* http://www.nytimes.com/2005/04/27/politics/27passport.html.

seven broad uses set out by DHS.[22] A "routine use" is a catch-all loophole in the Privacy Act that allows an agency to disclose personal information to others without the individual's consent.[23] The seven proposed uses, are:[24]

1. Disclosure to local, state, federal, tribal or foreign government agencies or organizations engaged in collecting law enforcement or intelligence information "and/or charged with investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders."

2. Disclosure in court, grand jury, or adjudicative body proceedings when records are determined by DHS to "be arguably relevant to the proceeding where any of the following is a party: (1) The DHS, or any DHS component, or subdivision thereof; (2) any DHS employee in his or her official capacity; (3) any DHS employee in his or her individual capacity when the DHS has agreed to represent the employee or has authorized a private attorney to represent him or her; and (4) the United States, where the DHS or its components are likely to be affected.

3. Disclosure "to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record."

4. Disclosure to the "National Archives and Records Administration or other Federal government agencies in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906."

5. Disclosure to the "news media and the public when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of the Department or is necessary to demonstrate the accountability of the Department's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy."

6. Disclosure to "contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records."

7. Disclosure to "an agency, organization, or individual for the purposes of performing authorized audit or oversight operations."

[22] 70 Fed. Reg. at 38700.
[23] 5 U.S.C. 552a(b)(3) (2004).
[24] 70 Fed. Reg. at 38700, 38701.

These broad exemptions clearly contravene the stated intent of the AIDMS. If the purpose of this record system is to facilitate processing for entry and exit at Points of Entry for the United States, then the additional purpose set out above are unnecessary and exceed the purpose of the record system. Accordingly, we urge that Department to revise the rule and remove these proposed routine uses.

Conclusion

For the foregoing reasons, EPIC urges the Department of Homeland Security to abandon the use of RFID technology in its I-94 forms; or, in the alternative, to delay such use until current privacy and security risks are eliminated.

Respectfully submitted,

_____
Cédric Laurant
Director, International Privacy Project

_____
Melissa Ngo
Staff Counsel

_____
Louisa Garib
Law Clerk

_____
Ibrahim Moiz
Law Clerk

ELECTRONIC PRIVACY INFORMATION

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