DEPARTMENT OF HOMELAND SECURITY
Privacy Office

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

---

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

On August 4, 2005, the Department of Homeland Security ("DHS") published notice that it would be testing the use of a radio frequency identification (RFID) tag with a unique identifier in its United States Visitor and Immigrant Status Indicator Technology program ("US-VISIT").[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. Individuals subject to US-VISIT are required to provide fingerscans, photographs, or other biometric identifiers upon arrival in, or departure from, 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."[2] "The 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."[3]

---

[1] Notice with request for comments, 70 Fed. Reg. 44934 (Aug. 5, 2005) *available at* http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve (hereinafter "August 2005 Notice").
[2] *Id.*
[3] *Id*.

In August 2005, the Electronic Privacy Information Center ("EPIC") submitted comments about the Automated Identification Management System ("AIDMS") system of records.[4] 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."[5] At that time, EPIC urged DHS to reject the use of RFID technology in its US-VISIT program.

Pursuant to the most recent notice, EPIC submits these comments to again 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, in the alternative, to delay such use until the findings of ongoing RFID testing are released and current privacy and security risks are eliminated.

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.[6] Next, we warned DHS that, in its continued implementation of US-VISIT, it must further protect against the dangers of

[4] 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.
[5] 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.
[6] 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.

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.[7] As we did in August 2005, we now urge that the Department of Homeland Security reject this proposal to incorporate a "contactless" RFID tag in the form I-94 and I-94W.

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. The data transmitted by the tag may provide identification or location information."[8] 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.[9]

According to the August 5, 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. When travelers either drive or walk through the port-of-entry to leave the United States, the transceivers 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

[7] 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.
[8] EPIC's Radio Frequency Identification (RFID) Systems page, *available at* http://www.epic.org/privacy/rfid/.
[9] 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.

> code number, when received by the transceivers, will be relayed back to secure DHS computer systems and matched with the biographic and/or biometric data of the traveler. 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.[10]

The Department of Homeland Security further explains that the US-VISIT program "will test the optimal distance at which the tag can be read during the traveler's exit and any subsequent re-entry and the tag's effectiveness and accuracy."[11]

DHS is aware that the use of RFID tags in this context raises security and privacy risks, and chose to use passive RFID tags (ones without their own power supplies, unlike active RFID tags) to mitigate these risks. However, the use of either passive or active RFID tags in I-94 forms still 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.[12] The ID number is the key that permits access to records in the US-VISIT system. As the notice states, "the DHS-issued RFID tag [will] transmit back a unique identifier code number. This code number, when received by the transceivers, will be relayed back to secure DHS computer systems and matched with the biographic and/or biometric data of the traveler."[13]

By their very design RFID tags, whether passive or active, 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

[10] August 2005 Notice at 44396, *supra* note 1.
[11] *Id*. at 44395.
[12] *Id*. at 44396.
[13] *Id*.

travelers carrying around RFID passports are broadcasting their identity."[14] This demonstrates another 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."[15] 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.

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

[14] Bruce Schneier, Opinion, *Passport radio chips send too many signals*, Int'l Herald Tribune, Oct. 4, 2004.
[15] August 2005 Notice at 44397, *supra* note 1.

made personal data contained in hi-tech passports vulnerable to unauthorized access.[16] 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, and DHS admits, that RFID tags can be read from thirty feet or more, posing a significant risk of unauthorized access.[17]

RFID is an invisible technology. It allows a person's information to be accessed without his or her knowledge. The slight timesaving 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 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 notice, the Department intends to test passive RFID tags that will "a*utomatically identify and document*" the entry and exit of covered individuals (emphasis added).[18] By design, this system will enable the surreptitious monitoring of

[16] 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.
[17] 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." August 2005 Notice at 44395 *supra* note 1; *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.
[18] August 2005 Notice at 44396, *supra* note 1.

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.[19] 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."[20]

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 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 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 raised by an RFID scheme lacking Basic Access Control. After the State Department received more than

[19] 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.
[20] *Id*. at 16.

2,400 comments on its notice for proposed rulemaking on RFID passports,[21] 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. [22]

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.

Conclusion

The stated goal of the RFID technology testing is to determine if the technology "can improve the efficiency of processing individuals who seek to enter or exit the United States at a land border port-of-entry."[23] The Department of Homeland Security has said, "Due to the significant cost associated with implementing exit control at all United States land border port-of-entry crossings, a full and comprehensive analysis of the proof of concept testing must be undertaken prior to any nationwide installation of radio frequency technology equipment."[24] We agree, and believe that a full and comprehensive analysis of the RFID proposal will show that the timesaving benefits of the proposal will

[21] 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.
[22] *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.
[23] August 2005 Notice at 44394, *supra* note 1.
[24] *Id*. at 44398.

be slight and significantly overshadowed by its privacy and security risks. For the foregoing reasons, we urge 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

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