

American Immigration Lawyers Association

918 F Street, N.W. Washington, D.C. 20004 (202) 216-2400

January 6, 2007

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

VIA Internet: <http://www.regulations.gov/index.cfm>

RE: 22 CFR PARTS 22 AND 51 RIN 1400 – AC 22 [PUBLIC NOTICE 5558]
CARD FORMAT PASSPORT; CHANGES TO PASSPORT FEE SCHEDULE

AGENCY: STATE DEPARTMENT

ACTION: PROPOSED RULE

Dear Sir or Madam:

The American Immigration Lawyers Association (AILA) submits these comments on the Proposed Rule published in the *Federal Register* on October 17, 2006 by the U.S. Department of State (referred to below as the Department or DOS). The Department's proposal announces the intended use of Radio Frequency Identification (RFID) technology, in particular, RFID Vicinity Read Technology (RFVRT), for passport cards to be used by U.S. citizens returning to the United States by land (from Mexico or Canada) and by sea (if travel has been between the United States, Canada, Mexico, the Caribbean or Bermuda).

AILA is a voluntary bar association of more than 10,000 attorneys and law professors practicing and teaching in the field of immigration and nationality law. Our mission includes the advancement of the law pertaining to immigration and nationality (including U.S. citizenship) and the facilitation of justice in the field. We appreciate the opportunity to comment on the Proposed Rule and believe our members' collective expertise provides a real-world basis that makes us particularly well-qualified to offer views which will benefit the public and the government. AILA members regularly advise and represent American companies and U.S. citizens who seek immigration benefits, including admission to the United States, and we provide counsel on other aspects of compliance with U.S. immigration, nationality and citizenship laws and regulations.

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22
January 6, 2007
Page 2

AILA recognizes the vital importance of enhancing our nation's security. We also believe that our government must protect the homeland in a way that balances the nation's need for enhanced security with improvements in the cross-border flow of people and goods (a cornerstone of the economic security that pays for our national security). AILA has consistently supported legislation to expand staffing for America's ports of entry and to ensure that inspection posts are otherwise well-equipped. For example, AILA strongly supported the Enhanced Border Security Act. The goal of this law is to make our borders a strong line of defense. To that end, the Act authorizes increased funding for immigration and border functions, requires federal agencies to coordinate and share information needed to identify and intercept terrorists; encourages the use of new technologies by authorizing funds to improve technology and infrastructure for immigration functions, targeting much of this effort at strengthening our nation's borders; mandates the transmittal of advance passenger lists; and mandates a study to determine the feasibility of a North American Perimeter Safety Zone. (This study would include a review of the feasibility of expanding and developing pre-clearance and pre-inspection programs.)

As A "Significant Regulatory Action" Under Executive Order 12866, The Proposed Rule Must Be Subjected To A Probing Cost/Benefit Analysis Prior To Final Promulgation

In the Supplementary Information accompanying the Proposed Rule, DOS asserts – incorrectly, AILA believes – that interagency analysis under Executive Order (EO) 12866 is not required. Although acknowledging that the proposal “does have important public policy implications,” and therefore has been submitted to the Office of Management and Budget (OMB) for an unspecified form of review, the Department wrongly concludes that there are no potential costs or consequences associated with the rule that would impose an annual effect on the economy of \$100 million or more.

The Department's decision to dispense with EO-12866 review is unsubstantiated and incorrect, given that the Proposed Rule does not consider the impact of passport-card user fees and the probable consequential impact on travel and trade. A simple calculation establishes the point. If the \$20 adult application fee and the \$25 execution fee are totaled (\$45) and at least 2.3 million adult U.S. citizens who are first-time applicants apply each year for the RFID-enabled passport card, the impact on the economy would exceed \$100 million.¹ Even more fundamentally, DOS fails to provide a cost-benefit analysis addressing the passport card's potential impact on border economies, on the

¹ The annual estimate of at least 2.3 million adult applicants for the passport card is reasonable, AILA believes, given the estimate in the prefatory comment to the Proposed Rule which notes that “Passport Services [projects] . . . an expected total of 12-12.5 million [passport applicants] in fiscal year 2006”.

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 3

travel and tourism industry, and on overall U.S. international commercial interests. Therefore, the ultimate cost and impact of the Proposed Rule remains undefined.

The Selection Of RFVRT For The Passport Card Has A Potential Adverse Effect On The Free Flow Of Travel And Trade

In general, AILA supports alternatives to passports for denoting identity and citizenship to enter the United States and other countries. AILA recognizes that the challenge at U.S. borders and ports of entry is how to assess individual travelers, based on the documents they present, without significantly slowing the processing time for admission into the United States. However, AILA is concerned that the creation of another identity document that cannot be used for all modes of travel might not ultimately be cost effective for the end user, that it might not necessarily provide for an easier or quicker means of moving traffic, and, that the confusion that will result from having a limited-use identity document could be counterproductive and may actually hinder the travel efforts of U.S. citizens.

In the Supplementary Information to the proposed rule, the Department notes that the proposed passport card is not intended to be a globally interoperable travel document as defined by the international Civil Aviation Organization (ICAO), and as such, is not suitable for wide use, including air travel. Because of the limited function of the passport card, another concern is the potential confusion that could result from U.S. citizens being able to obtain either document or both the passport and the passport card, documents whose names are similar but whose functions are not. It is easy to imagine the traveler who possesses both documents but takes the wrong one to the airport. It is also conceivable that individuals will misconstrue the limited use of the passport card and they will unknowingly obtain it, rather than a traditional passport, only to find that they are unable to embark on their anticipated travel because they possess the wrong type of document. And, one can envision the intended passenger whose travel plans change and who must fly home rather than return by land or sea, as was intended at the beginning of the journey. Such an individual could potentially be denied entry and/or delayed much longer than ever anticipated.

In addition, for admission at land ports of entry, such as for travel by car, if more than one passenger is in a vehicle, the effectiveness of the card will be diminished greatly. It is possible, and perhaps likely, that not all individuals traveling together will possess the same type of identity document. Once different passengers seek to produce different documents the anticipated speed and efficacy of having the cards will disappear. In fact, this situation may actually impede the speed of the inspection process because an officer will need to match each traveler to the individual's type of document and the questioning that will result will take longer than if all were to have just presented the traditional

RE: Card Format Passport; Changes to Passport Fee Schedule

RIN 1400-AC22

January 6, 2007

Page 4

passport in the first place. (A more thorough discussion of the inadequacies of the proposed passport card format for the tracking of individuals is discussed below.)

The Selection Of RFVRT – An Untested Technology In Human Tracking – Is Not Required By IRTPA

Aside from the unspecified but probably substantial impact of these newly required user fees and the adverse effect on the free flow of travel and trade, AILA believes that the Proposed Rule, if promulgated as suggested, would also threaten the security of the United States, and the privacy and security of the American people.

As a preliminary matter, we note that Congress has not mandated that the passport card carry a Radio Frequency (RF) capability or utilize some other technological approach. Specifically, Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108–458, 118 Stat. 3638 (Dec. 17, 2004), provides that U.S. citizens and nonimmigrant aliens may enter the U.S. only with passports or such alternative documents as the Secretary of Homeland Security may designate as satisfactorily establishing identity and citizenship. The statute requires that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement a plan to require virtually all travelers entering the U.S. to present a passport, other document, or combination of documents, that are “deemed by the Secretary of Homeland Security to be sufficient to denote identity and citizenship.”

The Use Of Untested RFVRT In Passport Cards Creates Unacceptable Risks To The Privacy, Security And Safety Of American Citizens

The Preamble to the Proposed Rule takes pains to emphasize the supposed benefits and privacy protections of RFVRT. According to the Department, RFVRT “would allow passengers approaching a land crossing in vehicles” apparently from as far away as 20 feet “to present the passport card to the reader easily from within the vehicle and these readers could process information from up to eight cards at one time.” A recent Government Accountability Office (GAO) report reveals that this assumed benefit, which DOS makes in order to justify the use of RFVRT in the passport card, is completely unwarranted.

Specifically, the GAO recently issued a report entitled **US-Visit Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry**² which documents extraordinarily dismal results regarding the use of RFVRT technology for human identification at land ports of entry. For example, at page 48, the report documents

² (GAO-07-248, December 2006), accessible at: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-248>

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 5

that the RFVRT technology in place at land ports provided a correct “read” rate in situations mirroring the entry process as set out in the proposed rule (and as quoted in the immediately preceding paragraph) of as low as a mere 14% where passengers in vehicles were involved.³

Moreover, in its proposed rule DOS also offers what the agency sees as an adequate privacy safeguard, namely, the storing and transmission of “only a unique reference number that will serve as a link to information safeguarded in a secure database managed by CBP [the Bureau of Customs and Border Protection].”

The DOS proposal, however, does not describe the data-privacy and -security precautions to be taken in transferring data maintained by the Department on passport applicants and issuances to the CBP-managed database at the ports of entry, or, how a CBP officer could conceivably review in any meaningful way the linked personal records of as many as eight passengers in a crowded minivan. Nor does the DOS address the possibility that a “unique reference number” could be read, for example, by a scanner from an adjacent vehicle queuing up at the land border or by a terrorist on a Caribbean cruise ship intending to target and harm U.S. citizens.

The Use Of RFID Technology For Human Tracking Is Facing Strong Criticism After Evaluation By Key Bodies Within The Department Of Homeland Security, The National Institutes Of Standards And Technology, And The Government Accountability Office

A. The DHS Data Privacy and Integrity Advisory Committee Voices Serious Concerns in the Use of RFID for Human Tracking.

A December 6, 2006 report from experts in the uses of RFID technology documents serious concerns with the potential use of RFID technology in documents such as the passport card. The report, **The Use of RFID for Human Identification**⁴, prepared for the Department of Homeland Security (DHS) Data Privacy and Integrity Advisory Committee by the Emerging Applications and Technology Subcommittee, highlights

³ Beyond the instant RFID operations issue, GAO has identified other performance and reliability issues related to passive RFID. For example, in June 2005 GAO testified before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security on similar reliability issues with RFID. It noted that when an object close to the reader or tag interferes with the radio waves, read-rate accuracy decreases, and that environmental conditions, such as temperature and humidity, can make tags unreadable. It further noted that tags read at high speeds have a significant decrease in read rates. See GAO, **Information Security: Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology**, GAO-05-849T (June 22, 2005).

⁴ The report may be accessed at:

http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 6

serious concerns with the potential use of RFID technology in tracking persons rather than mere merchandise. In using RFID in tracking persons, the Executive Summary of the report notes:

[T]here are a variety of concerns about the use of such systems, including:

- The potential for unauthorized access to the data on the RFID-enabled device, or the data when in transit between the device and reader;
- The selection of RFID-enabled systems for an application if other existing and potentially less privacy-impacting alternatives can achieve the same benefit;
- The concern that the information produced by an RFID-enabled credential system for a stated purpose might be reused or leveraged for a second purpose without the knowledge or consent of those persons whose information was collected for the original purpose;
- The concern that the deployment of RFID-enabled systems represents the potential for widespread surveillance of individuals, including US citizens, without their knowledge or consent.

AILA agrees with the report's authors who conclude that RFID technology will not accelerate the verification of identity and citizenship at ports of entry. The DHS report indicates that the perceived benefits in using RFID as a means of identifying humans are illusory. The report (at page 4) states:

RFID is a rapid way to read data, but RFID in a credential merely identifies the credential, not the individual bearing it. One or more biometric identifiers can be used to improve identification of human beings, but the steps needed to verify the biometric information using today's technology may reduce or negate the speed benefit offered by radio transmission.

[emphasis added]

After documenting potential security and privacy threats involved in the use of RFID technology, the report, at page 14, concludes:

The Committee recommends that the Department of Homeland Security carefully weigh the considerations detailed in...this Report before deciding to deploy an RFID-enabled system to identify individuals. An RFID-enabled system should be secure, narrowly-tailored to effectively accomplish a Department objective, and the least intrusive to privacy and security in light of alternative technologies to accomplish that objective. Otherwise, the use of RFID, standing alone, may not be best suited for purposes of identifying individuals and other solutions should be

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 7

considered. The Committee further recommends that if the Department determines to deploy an RFID-enabled system to identify individuals, that it build in, from the design stage, the safeguards outlined in...this Report to the extent possible to ensure that the use of RFID-enabled systems advance the Department's mission objectives while respecting and protecting the privacy and security of information collected about individuals.

Although addressed to DHS, the Committee recommendations are equally applicable to DOS uses of RFID technology for human identification. In respect to the proposed passport card, DOS has not undertaken the type of analysis recommended in the Committee report (or if one has been conducted, has not published any results). Accordingly, RFID technology should not be incorporated into the card and the Department should withdraw this ill-considered proposal until definitive research and analysis proves that RFID and RFVRT are suitable (on the basis of efficacy, privacy and data security) for use at ports of entry.

B. National Institute of Standards and Technology Questions the Viability of RFID for Human Tracking.

The National Institute of Standards and Technology (NIST), widely recognized for establishment of standards for use of specific technologies, has also recently addressed the serious potential vulnerabilities of RFID systems used for identifying and authenticating persons. In its recently published Special Publication 800-98 (Draft), **Guidance for Securing Radio Frequency Identification (RFID) Systems**,⁵ the NIST pointed out that such RFID systems can be easily compromised in the type of environment that exists at border crossings. The NIST report discusses the serious potential vulnerabilities of RFID systems used for authenticating persons, and points out that such systems can be easily attacked. In particular, the NIST report outlines four major categories of risk: business process risk, business intelligence risk, privacy risk, and externality risk. Before widespread implementation of RFID technology to authenticate people at border crossings, DOS must demonstrate that it has mitigated each of these risks, and that the new RFID system presents a lower risk in all of these areas than the traditional book-passport system it is replacing.

For example, the NIST report points out that "human threats" to RFID tags "include the ability of an adversary to damage or destroy a tag, remove the tag from the item to which it was attached, replace a tag with another one, or clone a tag and use the clone for an unintended purpose" (p. 3-9). Before implementing a final rule, DOS must explain how

⁵ See the draft report at: <http://csrc.nist.gov/publications/drafts/800-98/Draft-SP800-98.pdf>.

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 8

U.S. border security systems will overcome these “human threats” when the tags will not be under DOS’s control most of the time. The NIST report states that “human threats are more likely to be realized if outsiders (e.g., customers or members of the general public) have physical access to the tags and therefore the means to engage in malicious behavior. Human threats are more likely if people have an incentive to perform the attack, such as some form of financial gain or access to a restricted source” (p. 3-10). If one uses this analysis, AILA is hard pressed to conceive of a more vulnerable environment than that of “border security”, because it is well-documented that people will go to extraordinary lengths to enter the United States (even if that requires impersonation of U.S. citizens).

The NIST report also observes:

[RFID technology] represents a new attack vector on an enterprise network. Once RFID systems are implemented, a possibility exists that attackers could reach non-RFID and enterprise subsystem computers through an interrogator . . . Once RFID servers are compromised, they can be used to launch attacks on other networked systems . . . Once additional systems are compromised, all types of adverse consequences to the IT infrastructure are possible, including loss of confidentiality, integrity, and availability (p. 4-7).

The NIST report also notes that the risk of an enterprise-network attack is currently considered to be low, but "such a breach is inevitable, especially as RFID technology proliferates." (p. 4-7). DHS computer systems have in the past been successfully targeted by computer hackers, and remain highly vulnerable to future attacks.⁶ Before RFID systems are adopted in the border-security context, DOS and DHS must explain how these agencies have eliminated the risk that RFID technology might be used to attack government computer networks and gain access to the personal information of millions of Americans. DOS and DHS must also explain how implementing an RFID system will be more cost-effective than making marginal improvements to existing systems.

C. The Government Accountability Office Expresses Concerns about the Specific RFID Technology Standard Chosen by the DOS.

AILA also believes that the risks arising with RFID technology generally are multiplied with the use of specific RF technology proposed by the Departments. In its proposed

⁶ See “The Virus that Ate DHS” by Kevin Poulson, Wired Magazine, November 2, 2006 (available at <http://www.wired.com/news/technology/0,72051-0.html>) for an account as to how documentation gained through the Freedom of Information Act reveal the US-VISIT computer system was disabled by a teenage Moroccan hacker.

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 9

regulation, DOS specifically proposes the use of RFID ISO/IEC 18000 6-C technology in the passport card. The Government Accountability Office (GAO), however, recently issued a report entitled **Information Security: Radio Frequency Identification Technology in the Federal Government**⁷ which raises a red flag on this technology standard. As with the other cited studies, the GAO report confirms that security and privacy issues arising from the potential use of RFID in human tracking remain unresolved. In particular, Appendix 4 of the GAO report notes that RFID ISO/IEC 18000 6 technology is designed for item management, and not for human identification. The report identifies two RFID ISO standards other than ISO/IEC 18000 6 that are designed for use in identification cards, but nowhere states that security and privacy issues have been resolved for these standards.

The DOS implicitly acknowledges the security weaknesses inherent in the use of RFVRT for the proposed passport card. Recognizing the weakness, the Department proposes to "... produce the card[s] and deliver them with a thin protective sleeve, which is designed to protect the card from unauthorized access." The proposal, however, does not address the potential for unauthorized access (including skimming and cloning⁸) when the card is removed from its sleeve at a port of entry for verification of identity and citizenship.

Moreover, the sleeve itself creates clearly foreseeable risks of increased traffic accidents and of hacking. Assuming passport cards (complete with sleeves) are used at land ports of entry, some drivers are likely to remove the sleeves as the vehicle approaches primary inspection, thus creating moving-traffic hazards that could cause serious injury or death to border crossers. It is also foreseeable that (as most consumers already have learned) protective sleeves wear out and will therefore be discarded, thereby leaving some travelers with "naked" (unprotected) passport cards that are ripe for the purloining of data.⁹ When this happens, travelers with unprotected passport cards become identifiable as Americans to terrorists, identity thieves and other criminals with access to RFVRT scanners. In a worst case scenario, terrorists could use a technology that identifies the proximity of an unprotected RF passport card to trigger bombs left in an area frequented by American travelers.

⁷ (GAO-05-551, May 2005), accessible at: <http://www.gao.gov/new.items/d05551.pdf>.

⁸ "Skimming" is the unauthorized extraction of data from an RFID-embedded device. "Cloning" is the unauthorized duplication of all data contained in an RFID device.

⁹ The Department's proposal offers no information on the type of sleeve to be provided other than to describe it as "thin" and "protective." Thus, the public has no way of knowing whether such sleeves will be suitably impermeable to hacking, be thin enough to fit within a standard-size wallet pocket, and be durable (and if so for approximately how long – in the Department's estimate – before the sleeve's shielding effect is lost). In addition, the Department has not stated whether it will offer replacement sleeves, and if so, at what price and by what means of distribution.

Office of Passport Policy
Bureau of Consular Affairs
U.S. Department of State

10

RE: Card Format Passport; Changes to Passport Fee Schedule
RIN 1400-AC22

January 6, 2007

Page 10

Conclusion

AILA commends the Department for considering innovative approaches to border management. Nevertheless, we believe that the Proposed Rule should be withdrawn because the proposed passport card will not be an acceptable globally interoperable travel document, leading to confusion, inconvenience, and delay; because there has not been an adequate assessment of the cost to implement the proposed passport card system; and because of its reliance on unproven technology whose efficacy for human tracking, data privacy and security has not been established by experts in government or industry;

Respectfully submitted,

AMERICAN IMMIGRATION LAWYERS ASSOCIATION

cc: Steven D. Aitken
Acting Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503
Facsimile 202-395-3888