COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

DEPARTMENT OF HOMELAND SECURITY; DEPARTMENT OF STATE

Docket No. USCBP–2007–0061
Proposed Rule: Documents Required for Travelers Departing From or Arriving in the United States From Within the Western Hemisphere

---

By notice published on June 26, 2007, the Department of Homeland Security ("DHS") and the Department of State ("DOS") seek to expand the number of individuals submitting passport information, which would be required "for U.S. citizens and nonimmigrant aliens from Canada, Bermuda, and Mexico entering the United States by land from Canada and Mexico, or by sea from within the Western Hemisphere."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the DHS and the DOS to reject the use of "vicinity read" radio frequency identification technology in the Western Hemisphere Travel Initiative ("WHTI") passport card, because of the substantial privacy and security risks. EPIC also urges the DHS and DOS to delay the implementation of the passport card requirement until the agencies can find solutions for the extraordinary delays, problems, costs and privacy issues.

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 DOS to

[1] Dep't of Homeland Sec. and Dep't of State, *Documents Required for Travelers Departing From or Arriving in the United States at Sean and Land Ports-of-Entry From Within the Western Hemisphere*, 72 Fed. Reg. 35091 (June 26, 2007) *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/pdf/07-3104.pdf. [Hereinafter *NPRM for Travel Documents*].

[2] *See generally* EPIC's page on Radio Frequency Identification (RFID) Systems, http://www.epic.org/privacy/rfid/.

abandon its proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access.[3] In August and October 2005, we urged the DHS to abandon long-range, unsecured 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] 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 DHS Data Privacy and Integrity Advisory Committee.[5] In January, we urged the DOS to reconsider this proposal to use "vicinity" RFID technology in the WHTI passport card.[6] And, in May 2007, EPIC and 24 experts in privacy and technology submitted comments on DHS's draft implementation regulations for the REAL ID Act (which included a discussion of RFID technology use), saying that the plan would create new security risks for the American public.[7] Now we write again to urge you to reconsider the use of "vicinity read," also known as long-range, RFID technology and to delay implementation of WHITI until the documented delays, problems, costs and privacy concerns are addressed.

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

---

[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, *Comments on Docket No. DOS-2006-0329: Proposed Rule: Card Format Passport; Changes to Passport Fee Schedule* (Jan. 8, 2007) available *at* http://www.epic.org/privacy/rfid/whti_010807.pdf; 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] EPIC, *Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

be transparent in their information practices.[8] 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, 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.[9]

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[.]"[10] 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."[11] 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.[12] Adherence to these requirements is critical for a system such as the passport card, which would be required for millions of American citizens and lawful permanent residents who travel to Canada, Mexico, the Caribbean and Bermuda.[13]

The Intelligence Reform and Terrorism Prevention Act of 2004 mandated that, by

---

[8] S. Rep. No. 93-1183 at 1 (1974).
[9] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[10] S. Rep. No. 93-1183 at 1.
[11] Pub. L. No. 93-579 (1974).
[12] *Id*.
[13] Press Release, Dep't of State, *Department of State to Introduce Passport Card* (Oct. 17, 2006) *available at* http://www.state.gov/r/pa/prs/ps/2006/74083.htm.

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 countries in North, Central or South America.[14] This program is called "WHTI," 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 passport card.[15] This is a significant change from the current practice in which U.S. citizens 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.[16]

The notice of proposed rulemaking states that a "Privacy Impact Assessment (PIA) is being posted to the DHS Web site in conjunction with the publication of this proposed rule in the Federal Register."[17] The notice for proposed rulemaking was released on June 26, 2007; however, as of July 26, 2007, the PIA was still not released. This is a disturbing trend for DHS and frustrates meaningful public comment, which is the purpose of the Administrative Procedures Act. Linda Koontz, Director of Information Management Issues at the Government Accountability Office, testified in July 2007 that "the Privacy Office has generally not been timely in issuing public reports."[18] In fiscal year 2005, DHS identified 46 systems that needed a PIA, and in fiscal year 2006 DHS identified 143 such systems. However, only 20 of the 48 PIAs required were published in fiscal year 2005 and only 25 of the 143 required PIAs were published

[14] Pub. L. No. 108-408, §7209, 118 Stat. 3638, 3823 (2004).
[15] Dep't of State, *Card Format Passport; Changes to Passport Fee Schedule*, 71 Fed. Reg. at 60928 (Oct. 17, 2006),
[16] Frank Moss, Deputy Assistant Sec. for Passport Services, Bureau of Consular Affairs, Dep't 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.
[17] *NPRM for Travel Documents*, *supra* note 1 at 35112.
[18] Statement of Linda Koontz, *Testimony Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives*, at 3 (July 24, 2007) *available at* http://www.gao.gov/new.items/d071024t.pdf.

in fiscal year 2006, demonstrating the continuing troubles DHS has had fulfilling its privacy obligations. The Privacy Office estimates 188 systems will need a PIA in fiscal year 2007, but the Privacy Office's dismal history makes it likely that the Office will not fulfill its obligations.[19]

The Homeland Security Act requires the Chief Privacy Officer to report its activities, including complaints of privacy violations, to Congress annually.[20] "However, the office has issued only two annual reports within the 3-year period since it was established in April 2003, and one of these did not include complaints of privacy violations as required," according to Koontz's testimony.[21] Not only does this erode the Privacy Office's credibility, but it also "hinders the public's ability to understand the nature of DHS systems-of-records notices and how their personal information is being used and protected," Koontz said.[22] Without the required Privacy Impact Assessment, it is difficult to really know the full extent of the privacy implications regarding the WHTI system designed by DHS and DOS.

I. Delays and Problems Issuing Passports Are Not Abating

On January 23, the government implemented new rules requiring more Americans to have passports when traveling to Canada, Mexico, Bermuda and the Caribbean. "By summer, more than 2 million Americans were waiting for passports; half a million had waited more than three months since applying for the travel identification that historically has been ready in six weeks."[23] Because of this backlog, DHS postponed the WHTI requirement in June 2007.[24]

Although DHS was responsible for the massive change in document requirements for

---

[19] *Id*.
[20] Homeland Security Act of 2002, Sec. 222, Pub. L. No 107-296 (Nov. 25, 2002).
[21] Statement of Linda Koontz, *Testimony Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives*, *supra* note 18 at 3, 4.
[22] *Id*. at 19.
[23] Associated Press, *Official takes blame for passport mess*, July 23, 2007 http://www.cnn.com/2007/TRAVEL/07/23/passport.mess.ap/index.html
[24] Press Release, Dep't of State, *Travel Accommodation Announced June 8, 2007* (Jun. 8, 2007) *available at* http://travel.state.gov/travel/cbpmc/cbpmc_2223.html.

U.S. travelers, Assistant Secretary of State Maura Harty, who is in charge of passports for U.S. citizens, recently took the blame for the backlog, which has lead to numerous stories documenting individuals' ruined travel plans. Some of the reasons for the delays in processing passports have been "inept planning, underfunded preparations, popular misunderstanding of poorly crafted government advertising, unanticipated effects of public debate over immigration, tardy and ill-considered responses to the developing crisis, and even partly […] Hurricane Katrina, which damaged the New Orleans processing office."[25]

II. These Delays Are Harming, Not Helping, National Security

Beyond the fact that the passport delays are costing U.S. citizens time and money by causing them to stand in unusually long lines, call their state and Congressional representatives, and miss vacations or business trips, national security is also being affected negatively by the WHTI proposal. There is a real question of whether requiring people to have passports or passport cards will increase national security. The assumption that any person with a passport or a passport card is not a terrorist is based on the flawed presumptions that terrorists do not qualify for these legal documents. However, evidence to the contrary is quite clear in incidents such as the 9/11 terrorist attacks where several hijackers had fresh passports.[26]

Another example showing that identification cards do not screen out wrongdoers or terrorists is the Florida baggage handler case. In this case, two men entered restricted areas in a Florida airport, bypassed security screeners and carried a duffel bag containing 14 guns and drugs onto a commercial plane."[27] They avoided detection, because they were airline baggage handlers who used their uniforms and legally issued identification cards. Both men had passed

[25] Associated Press, *Official takes blame for passport mess*, *supra* note 23.
[26] Elaine Shannon, *9/11 Hijackers: The Passport Scam*, TIME, Feb. 1, 2004 *available at* http://www.time.com/time/magazine/article/0,9171,1101040209-586213,00.html.
[27] Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*, Associated Press, Mar. 9, 2007.

federal background checks before they were hired, according to a spokesman for Comair, the airline that employed the men. The men were only investigated and caught after receiving an anonymous tip. As Bruce Schneier, chief technology officer at the security firm BT Counterpane, said, "This kind of thing is inevitable. Whenever you have a system that requires trusted people -- that is, every security system -- there is the possibility that those trusted people will not behave in a trustworthy manner."[28]

Another reason why requiring passports or passport cards will not increase national security is because such cards may be issued based on fraudulent documents. DHS said that people are currently "presenting fraudulent documents that cannot be validated; presenting facially valid documentation that cannot be validated against the identity of the holder."[29] These problems will still occur under the WHTI framework. For passport applicants, a previous U.S. Passport, certified birth certificate, consular report of birth abroad or certification of birth, naturalization certificate or certificate of citizenship can prove U.S. citizenship.[30] If an applicant does not have a previous U.S. passport or certificated birth certificate, the applicant can still prove citizenship by a letter of no record and "as many of the following as possible: baptismal certificate, hospital birth certificate, census record, early school record, family bible record, doctor's record of post-natal care."[31] An applicant must also provide proof of his or her identity through either a previous U.S. passport, naturalization certificate, or a current valid driver's license, government or military identification. If these are not available, then the applicant must

[28] Bruce Schneier, *Airport Credentials Manipulated to Commit Crime*, Mar. 13, 2007, http://www.schneier.com/blog/archives/2007/03/tia_credentials.html.
[29] *NPRM for Travel Documents*, *supra* note 1, at 35092. ("This refers to individuals who obtain valid documents through malfeasance. In such cases, the individual uses fraudulently obtained source/feeder documents to impersonate the U.S. or Canadian citizen in order to obtain the new document (*i.e.*, identity theft)).
[30] Dep't of State, *How to Apply in Person for a Passport*, Bur. of Consular Affairs, http://travel.state.gov/passport/get/first/first_830.html.
[31] *Id*.

bring documents that contain signatures and "a person who can vouch for you."[32] Many of these documents can be forged and therefore passports can be issued on false documentation, which creates a system where the legitimacy of valid passports could be eroded.

This is not mere supposition. In August 2005, the Government Accountability Office (GAO) investigated and found errors in information from Department of Homeland Security databases.[33] A December 2006 report from the Social Security Administration's Office of Inspector General found problems in databases of Citizenship and Immigration Services.[34] The report documented accuracy problems in the Social Security database Numerical Identification File (NUMIDENT), which also is used to check employment eligibility status. The Inspector General estimated that about 17.8 million records in NUMIDENT have discrepancies with name, date of birth or death, or citizenship status.[35] About 13 million of these incorrect records belong to U.S. citizens.[36]

With the increase of passport applications -- there are an expected 17.5 million applications in 2007 -- there is a question as to whether adjudicators are given enough time to "thoroughly check applications; others say the databases used to verify an applicant's identity and eligibility are incomplete."[37] Despite expanding the information passport adjudicators need to look at before issuing a passport,[38] "[a]djudicators have, on average, 2-1/2 minutes to evaluate

---

[32] *Id*.
[33] Gov't Accountability Office, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO-05-813 29 at 25 (Aug. 2005) *available at* http://www.gao.gov/new.items/d05813.pdf.
[34] Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's Numident File, A-08-06-26100*, at 15 (Dec. 18, 2006) *available at* http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.
[35] *Id*. at 6.
[36] *Id*. at Appendix C-2.
[37] Zoe Tillman, *Are new passport rules making the US safer?*, Christian Science Monitor, July 24, 2007 http://fe29.news.sp1.yahoo.com/s/csm/20070706/ts_csm/apassports.
[38] For example, passport adjudicators have to cross-check the applicant with a database of people who are behind in child support payments through the Department of Health and Human Services.

an applicant's eligibility for a passport."[39]

Even if each passport or passport card is meticulously checked, this still does not mean that these forms of identification will increase national security.[40] "There's a pervasive myth that if we only knew who everybody was, we could pick out the bad guys," said security expert Bruce Schneier. Knowing who intends to do harm is really the key "and a better ID won't help with that."[41] Schneier also "notes that Oklahoma City bomber Tim McVeigh, the London subway bombers, and even some of the Sept. 11 terrorists did not have fake IDs."

III. Cost of WHTI Mandate in Money and Implementation is Prohibitive

Though the price of an individual passport or passport card itself is not prohibitive, there are other costs to consider.[42] 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 passport card.

There are costs for the reader equipment. Estimates place the cost to implement the passport card at $406 million annualized (7 percent discount rate).[43] In May 2006, the GAO found that "not all land ports of entry currently have equipment to read documents [passport cards], and existing equipment may not be compatible with the approach chosen."[44] By the June 1, 2009, deadline DHS and DOS "anticipate that RFID infrastructure will be rolled out to cover

---

[39] Zoe Tillman, *Are new passport rules making the US safer?*, *supra* note 37.
[40] *See generally*, Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec.* (Mar. 21, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.
[41] Michael J. Sniffen, *She Takes the Blame for Passport Mess*, Associated Press, July 22, 2007 *available at* http://news.aol.com/story/_a/she-takes-the-blame-for-passport-mess/20070722100409990001.
[42] Dep't of State, Bureau of Consular Affairs, *Passport Fees,* http://travel.state.gov/passport/get/fees/fees_837.html.
[43] *NPRM for Travel Documents*, *supra* note 1, at 35109. When calculating costs and benefits that occur over a series of years, it is generally accepted that future costs and benefits should be discounted as a result of the time value of money. A higher discount rate reduced the weight of future costs and benefits. Discount rates reduce the relative value of future benefits, or may result in a more favorable evaluation.
[44] Gov't. 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.

the top 39 ports-of-entry (in terms of number of travelers) through which 95 percent of the land traffic enters the United States."[45] However, all of "the remaining land and all sea ports-of-entry would utilize existing machine-readable zone technology to read the travel documents."[46] Therefore, a large number of land ports would need to be updated with technology capable of reading RFID chips. This would cost an enormous amount of time and money.

There are costs of reporting and record keeping for passport cards as well. The increase in the number of individuals who would need to apply for passports or the proposed passport cards, also increases the required annual reporting. DHS and DOS have estimated annual average reporting and record keeping at 14.7 million hours.[47] The agencies estimated that there would be 9 million annual respondents.[48]

There are also costs to U.S. citizens in terms of international trade. For example, Sen. Patrick Leahy has explained that WHTI would significantly affect his state of Vermont. 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."[49] There are concerns about the effect WHTI would have 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," Leahy said.[50]

Sen. Hillary Rodham Clinton from New York also said that WHTI would negatively affect her state's economy. She said:

---

[45] *NPRM for Travel Documents, supra* note 1, at 35092.
[46] *Id*.
[47] *Id*. at 35111. Research did not yield historic data to compare to these new numbers.
[48] *Id*.
[49] Statement of Sen. 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.
[50] *Id*.

> The exchange of goods between the United States and Canada is the largest trading relationship in the world. On average, $1.1 billion in goods cross the border each day. This number is likely to decrease dramatically if an individual is forced to purchase a $45 passport card - or an even more expensive passport - several weeks in advance in order to cross the border. A decrease in cross-border travel would be devastating to the economies of both the U.S. and Canada. The impact would cripple border communities such as the Buffalo-Niagara region in New York.[51]

Michigan will also feel the impact. According to Congressman Bart Stupak, "[c]ommerce and trade between the U.S. and Canada is an economic engine that generates upwards of $400 billion per year for our country and supports over 170,000 Michigan jobs."[52]

Washington Senator Maria Cantwell said that the impact of WHTI could "cut off border communities, slow tourism, and deliver a damaging blow to our economy. With the 2010 Winter Olympics coming to Vancouver, we can't bring our border to a standstill. Our economy depends on trade, tourism, and a border open to legitimate travel."[53]

Many Canadian representatives and groups have spoken out against the WHTI mandate. The Canadian Tourism Commission said, "[a] recently released Industry Canada study projects the WHTI could result in a loss of over 14 million inbound trips from the US and a loss of $3.6 billion in tourism receipts between 2005 and 2010."[54] BESST, a coalition of Canadian and U.S. businesses and trade associations, have estimated that "Washington County Maine will lose 1.41% of its employment, and Whatcom County, Washington will lose 0.53% of its employment.

---

[51] Letter from Sen. Hillary Rodham Clinton to Sec. of State Condoleezza Rice and Sec. of Dep't of Homeland Sec. Michael Chertoff (Mar. 22, 2007) *available at* http://www.senate.gov/~clinton/news/statements/record.cfm?id=271156.

[52] Press Release, Cong. Ne. Border Caucus, *Stupak, McHugh Call for Delay of New Passport Law*, (Feb. 21, 2007) *available at* http://www.house.gov/list/press/mi01_stupak/WHTILetter022107.html.

[53] Press Release, Sen. Cantwell, *Cantwell, Larsen Lead Effort to Enhance Security Without Slowing Legitimate U.S.-Canada Commerce and Travel*, (Jan. 25, 2006) *available at* http://cantwell.senate.gov/news/record.cfm?id=250729.

[54] Tourism staff, *WHTI will change how we do business*, 3 Tourism 11 (Nov. 2006) *available at* http://www.corporate.canada.travel/corp/media/app/en/ca/magazine/article.do?issuePath=templatedata%5Cctx%5CmagIssue%5Cdata%5C2006%5Cissue11%5Cissue2006_11&path=templatedata%5Cctx%5CmagArticle%5Cdata%5Cen%5C2006%5Cissue11%5Cnews_and_opinion%5Cwhti.

For Whatcom County, that would mean over 500 people will lose their jobs."[55] Perhaps even more succinctly, Yukon State Rep. Jeff Morris said, "You would think that it should take less to cross the border between the United States and Canada then [sic] it did to go from West Berlin to East Berlin during the height of the Cold War."[56] These are only some of the states whose economies will be affected by WHTI mandate.

The DHS and DOS analysis of the economic impact of WHTI does not appear to take into account real life cost-benefit analysis when considering net expenditure flows in North America.[57] The report estimates that "[s]pending by U.S. travelers who forgo travel to Mexico" will keep approximately $440 million in the United States. This does not appear to take into account any cost-benefit analysis. One example would be individuals who cross the border to buy prescription drugs. A first-time passport costs $97, while a passport renewal costs $67.[58] However, people who travel to Canada to buy medication have reported buying "19 three-month prescriptions" saving "a total of $860."[59] The cost of spending $97 dollars for a document that will last for 10 years is negligible compared to the prescription drug savings people experience when crossing either border. The cost-benefit analysis in this situation infers that many people will pay the cost for a passport or a passport card so that they can continue to cross the border to get prescription drugs.

Lastly, some proponents of RFID technology have touted the decreased time that vehicles would need to wait during border crossings. In 2006, the highest average daytime wait on the

---

[55] Letter from BESTT Coal. to Dep't. of Homeland Sec. and Dep't. of State (July 12, 2007) *available at* http://www.besttcoalition.com/files/2007_NPRM_Response_FINAL.pdf.
[56] Press Release, Pac. NW. Econ. Region, *Zogby Poll Reveals Economic Impact of Passport Requirement*, (Mar. 17, 2006) *available at* http://www.gov.yk.ca/news/2005/06-053.html.
[57] *NPRM for Travel Documents*, *supra* note 1, at 35106.
[58] Dep't of State, *Passport Fees*, *supra* note 42.
[59] Lisa Gibbs, *Drug Trips While Washington Debates How to Make Medicines More Affordable, Many Americans are Going to Canada to get a Better Deal*, CNN Money.com (Sept. 1. 2001) http://money.cnn.com/magazines/moneymag/moneymag_archive/2001/09/01/308602/index.htm.

Canadian border was over 20 minutes at Blaine-Peace Arch, while the highest average daytime wait on the Mexican border was almost 50 minutes on the San Ysidro.[60] DHS and DOS used a baseline of 45 seconds for standard processing of documents.[61] Time estimates for border patrol agents to verify RFID enabled documents is 20 seconds, "machine readable zone" identification clocks in at 25 seconds, and for standardized documents can be verified in 30 seconds.[62] This report does not take into consideration that individuals may still need further evaluation, even after they have been identified as authentic border crossers. For example, border patrol agents must still inspect cars for contraband and agriculture, even if the passengers' documents have been verified. The report also noted that using RFID-enabled passports or passport cards "may increase the number of individuals sent to secondary inspection due to an increase in the number of database *hits*, or identifications, of criminals or individuals with immigration violations (whether true or false), particularly during the Implementation Stage."[63] In addition, the use of RFID technology "could require a moderately higher amount of energy for additional technology (such as RFID readers) and computer processing."[64] Thus, the claim that RFID would curtail energy concerns about cars idling for an additional 25 seconds is misleading. The privacy problems with RFID technology are not worth the possibility that RFID-enabled documents might save 25 seconds of wait time.

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

[60] Customs & Border Protection, *Western Hemisphere Travel Initiative in the Land and Sea Environments*, Draft Programmatic Environmental Assessment, at 27 (June 2007) *available at* http://www.cbp.gov/linkhandler/cgov/travel/alerts/whti_land_sea/whti_pea.ctt/whti_pea.pdf.
[61] *Id*. at 36.
[62] *Id*. at 37.
[63] *Id*. at 41.
[64] *Id*. at 55.

As stated in EPIC's previous comments on WHTI, there are significant privacy and security risks associated with the mandatory use of RFID-enabled passport cards to track the entry and exit of U.S. citizens.[65] The use of "vicinity" or "long-range" RFID tags enhances these threats.

In May 2007, EPIC's submitted detailed comments explaining the significant security and privacy problems in the WHTI program.[66] At that time we noted that DOS changed its E-Passport proposal because of security and privacy threats.

In 2005, DHS began testing RFID-enabled I-94 forms in its US-VISIT program to track the entry and exit of visitors.[67] The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitors' personal data.[68] EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards.[69] The DHS's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the

---

[65] EPIC, *Comments on Docket No. DOS-2006-0329: Notice of Proposed Rulemaking and Request for Comments*, *supra* note 6.
[66] *Id*.
[67] Dep't of Homeland Sec., *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*, 70 Fed. Reg. 44,934 (Aug. 5, 2005) *available a*t http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?dbname=2005_register&position=all&page=44934.
[68] The data includes biographic information, such as name, date of birth, country of citizenship, passport number and country of issuance, complete U.S. destination address, and digital fingerscans. Dep't of Homeland Sec., *Notice of Availability of Privacy Impact Assessment*, 70 Fed. Reg. 39,300, 39,305 (July 7, 2005) *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm.
[69] 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* (Dec. 8, 2005) *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

RFID-enabled I-94 forms.[70] In a January report, the GAO also identified numerous performance and reliability problems in RFID-enabled US-VISIT documents.[71]

The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9, 2007 that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.[72] The pilot test was a failure, in part, because, as the GAO report found, "[t]he RFID solution did not meet the statutory requirement for a biometric exit capability because the technology as tested cannot meet a key goal of US-VISIT – ensuring that visitors who enter the country are the same ones who leave."[73]

In December 2006, the Department of Homeland Security Data Privacy and Integrity Advisory Committee (DPIAC) adopted a report, "The Use of RFID for Human Identity Verification," which included recommendations concerning the use of RFID in identification documents.[74] The committee outlined security and privacy threats associated with RFID, and it urged against using RFID technology unless the technology is the "least intrusive means to achieving departmental objectives."[75] The long-range RFID-enabled passport card is not the least intrusive means. For example, an individual could hand the passport card to a border control

---

[70] Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006) *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf.
[71] Gov't Accountability Office, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry* (Jan. 31, 2007) at 4, *available at* http://www.gao.gov/new.items/d07378t.pdf.
[72] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't Of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007) *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.
[73] Gov't. Accountability Office, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, *supra* note 71 at 4.
[74] Dep't. of Homeland Sec., 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.
[75] *Id*. at 2.

official. The proposed passport card fails to comply with the DHS Data Privacy and Integrity Advisory Committee's recommendations regarding the use of RFID technology.

In Congressional testimony in March 2007, a GAO official cautioned against the use of RFID technology to track individuals. "Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's privacy," the GAO said.[76] The GAO reiterated the many problems with the failed US-VISIT RFID project and expressed concern that, despite this failure, DHS endorsed the use of RFID in the WHTI passport card.[77]

Privacy and security risks associated with RFID-enabled identification cards include "skimming" and "eavesdropping." Skimming occurs when an individual with an unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as an authorized RFID reader reads the data. Security expert 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."[78]

So long as unauthorized individuals can read the RFID tag or chip, the person carrying that tag can be distinguished from any other person carrying a different tag. Individuals, unlike commercial products with RFID tags, should have the right to control the disclosure of their identifying information.

---

[76] Linda D. Koontz, Dir., Info. Mgmt. Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Homeland Sec., H. Comm. on Appropriations*, 110th Cong. (Apr. 14, 2007) *available at* http://www.gao.gov/new.items/d07630t.pdf.
[77] *Id*. at 4.
[78] Bruce Schneier, *Passport radio chips send too many signals*, Int'l Herald Tribune, Oct. 4, 2004.

These privacy and security risks are contrary to the recommendation of the International Civil Aviation Organization ("ICAO"). ICAO had earlier proposed implementation of strong security features in all machine-readable travel documents.[79] 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."[80] Despite this recommendation and the many benefits of Basic Access Control, the proposed rulemaking does not mention Basic Access Control.

Under such a Basic Access Control system, 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 passport 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. However, the Basic Access Control solution does not 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 serious disregard of security

[79] 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.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf.
[80] *Id*. at 16.

and privacy safeguards, the agency said it would implement Basic Access Control that would prevent skimming and eavesdropping.[81] The RFID implementation proposed in the passport cards contravenes DHS's incorporation of basic security features into new U.S. passports.[82]

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 DOS does implement the long-range RFID-enabled passport card proposal, it should at least incorporate Basic Access Control or equivalent security features, into the cards.

In the absence of effective security techniques, RFID tags are remotely and secretly readable. Although the creation of a small, easily portable RFID reader may be complex and expensive now, it will be easier and less expensive as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches. In its now-abandoned US-VISIT pilot test, DHS said, "reliable reads can be received from a few inches to as much as 30 feet away from the reader."[83] Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.[84]

Some attacks already have succeeded against 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

---

[81] Notice of Proposed Rule, 70 Fed. Reg. 8305 (Feb. 18, 2005).
[82] *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.
[83] Dep't of Homeland Sec., *Notice with request for comments*, 70 Fed. Reg. 44,934, 44,395 (Aug. 5, 2005) *available at* http://frwebgate1.access.gpo.gov/cgibin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve.
[84] *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.

software that took him less than a couple of days to write.[85] 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 those researchers spent only a few weeks attacking the RFID-enabled passports.[86]

Another security risk of RFID-enabled identification cards is 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 identification card. The GAO 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.[87]

The DHS Data Privacy and Integrity Advisory Committee report on the use of RFID urged against RFID use unless the technology is the "least intrusive means to achieving departmental objectives."[88] It is clear that the costs of RFID technology outweigh its benefits, and it should not be used in identification documents.

Conclusion

The proposed WHTI passport cards would cost too much in terms of security and money. National security would be compromised as applications for these cards would create opportunities for forgery, opportunities which adjudicators are ill-prepared to handle. The cost of

---

[85] Steve Boggan, *Special Report: Identity Cards: Cracked It!*, Guardian, Nov. 17, 2006.
[86] Bruce Schneier, *The ID Chip You Don't Want in Your Passport*, Wash. Post, Sept. 16, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/09/15/AR2006091500923.html.
[87] Gov't 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.
[88] Dep't. of Homeland Sec., Data Privacy and Integrity Advisory Committee, *The Use of RFID for Human Identity Verification*, *supra* note 74 at 2.

the WHTI proposal is prohibitive to U.S. citizens for both the equipment infrastructure, and its effect on international trade. Furthermore, the long-range, unsecured RFID technology called for in the WHTI passport card proposal creates significant security and privacy risks. For the reasons stated above, EPIC urges the DHS and DOS to reject the use of long-range, unsecured RFID technology in the documents. In the alternative, if the agencies seek to move forward with the proposed passport cards, we urge the agencies to postpone the implementation of WHTI's new rules requiring individuals crossing U.S. borders to obtain new passports or passport cards until the problems explained above are solved.

Respectfully submitted,

_____
Marc Rotenberg
Executive Director

_____
Melissa Ngo
Senior Counsel

_____
Tanith Balaban
IPIOP Clerk

_____
Mark Pike
IPIOP Clerk

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

Filed: August 1, 2007