CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

January 7, 2007

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

Re: Comments on *Card Format Passport; Changes to Passport Fee Schedule*
Docket ID: DOS-2006-0393
22 CFR Parts 22 and 51
RIN 1400-AC22
[Public Notice 5558]

Dear Sir or Madam:

The Center for Democracy & Technology (CDT) appreciates the opportunity to provide comments on the PASS (People Access Security Service) Card, a joint project of the Departments of State and Homeland Security, and part of the Western Hemisphere Travel Initiative (WHTI) created by §7209 of the Intelligence Reform & Terrorism Prevention Act of 2004.[1]

CDT is a 501(c)(3) non-profit public policy organization dedicated to promoting the democratic potential of the open, decentralized, global Internet and related information technologies. Our mission is to develop and promote public policies to preserve and enhance free expression, privacy, open access, and other democratic values in the new and increasingly integrated digital communications networks. CDT has been a leading voice on privacy issues in identity systems and technologies. We convened the RFID Working Group, which developed privacy best practices for the deployment of RFID technology in the consumer

[1] Card Format Passport; Changes to Passport Fee Schedule, 71 Fed. Reg. 60928 (2006) (to be codified at 22 C.F.R. pts. 22 & 51) (proposed October 17, 2006) ("PASS Card Proposed Rule").

context. We also convened the Authentication Privacy Principles Working Group, which developed Privacy Principles for Authentication Systems.

I. SUMMARY

The Proposed PASS Card is intended to be used by American citizens who frequently travel by land or sea to Canada, Mexico, the Caribbean and Bermuda. In an effort at efficiency, the State Department has chosen to incorporate in the card a form of Radio Frequency Identification (RFID) technology. RFID tags were designed for use in tracking inventory. Passive tags are triggered remotely, and all RFID tags can be read at a distance by "readers" using radio signals, without the knowledge or consent of the person carrying the tag. RFID tags are becoming ubiquitous in the manufacturing-to-retail supply chain. The technology is based on public standards that emphasize speedy data capture and interoperability. RFID readers will become increasingly cheap and easy to build and deploy.

CDT is gravely concerned that the proposed PASS Card lacks adequate security and privacy protections. In the context of human identification, RFID technology should be deployed, if at all, only with scrupulous attention to privacy and security. In this case, the "vicinity read" RFID technology chosen by the State Department in the PASS Card Proposed Rule is inherently, indeed intentionally, insecure. When used for human identification, it poses threats to personal privacy and safety, including location tracking, "mission creep," identity theft and physical risks to Americans carrying the card. These risks are too great to move forward with the current proposal. CDT urges the State Department to fundamentally revisit the design of the PASS Card program. We outline below specific issues that should be examined.

The concept of information privacy involves, in part, the right of an individual to control how and when information about herself is disclosed and used. The use of an RFID tag in a human identification document implicates two kinds of privacy interests: control over personal information contained on the tag and in associated databases (data privacy), and control over the information regarding the individual's physical location and movement as determined by reading the tag (location privacy).[2] The design of the PASS Card fails to adequately protect either of these privacy interests.

The State Department made three key decisions in designing the PASS Card. First, it decided to make the PASS Card machine-readable, to facilitate the collection of data from the card and its comparison against information in a back-end database. This is consistent with other trends in ID card technology, and CDT has no objection to the use of machine-readable documents in the border-crossing context. Second – and this is where concerns begin to arise – the State Department chose RFID as its preferred machine-readable technology, favoring, for reasons that may not be valid, a technology that allows data to be read remotely, i.e., without contact between the card and the reader. Of the various machine-readable technologies available, RFID is not the

[2] Smart Border Alliance, *US-VISIT Increment 2C RFID Feasibility Study, Final Report*, *Attachment E: RFID Security and Privacy White Paper*, §3.0 (January 21, 2005) ("US-VISIT RFID White Paper") <http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf>. *See also id.* at §2.2 ("This security assessment focuses on an examination of risks inherent in RFID Systems employing Ultra-High Frequency Generation 2 (UHF Gen2) Standard passive tags").

best for human identification. Its use in the PASS Card would greatly reduce user notice and control over when information is collected from the card. Third, and fatally, the State Department selected a "vicinity read" or long-range GEN-2 RFID technology, which enables both data and location privacy to be compromised at considerable distances. Both long-range and short-range RFID tags are essentially two-way radios that can transmit signals over long distances and without line-of-sight. Because the long-range GEN-2 tag was not designed for human identification, it is inherently insecure and so definitely should *not* be used for the PASS Card.

Additionally, the policy justifications proffered by the State Department to support the long-range RFID technology choice are unpersuasive and certainly do not outweigh the serious privacy risks associated with the use of it in a human identification document. However, even the standard examined by the State Department for short-range tags seems to be inadequate. Indeed, it is expressly not a security standard. Like the long-range RFID system, a short-range RFID system is susceptible to skimming, eavesdropping and hacking, and a short-range RFID tag also can act like a beacon by revealing the presence of the PASS Card holder. The State Department's proposal that a protective sleeve be used with the PASS Card is an admission of the Card's security flaws. In contravention of sound "security-by-design" principles, it places the security burden on the PASS Card holder. And, in any event, the protective sleeve is useless against eavesdropping on an authorized transaction at the border when the card must be removed from the sleeve.

For these reasons, CDT urges the State Department to seriously consider for the PASS Card other machine-readable technologies that offer a higher degree of security and privacy. CDT recommends that the State Department conduct a detailed cost-benefit analysis to better understand the pros and cons of using RFID technology, compared to other machine-readable technologies.

As part of this process, the State Department and DHS should reconsider whether to move forward with the PASS Card program at all. The State Department and DHS decided to develop the PASS Card as a cheaper and faster alternative to the traditional passport, to facilitate cross-border border travel for those who frequently enter Mexico or Canada for work, family, recreation, and shopping. However, to make the PASS Card properly secure would increase the cost of the card, possibly to the point where it is not significantly less expensive than the passport book. In addition, there apparently has been no threshold study to quantify the efficiency benefits of contactless cards for border processing. CDT urges the Departments to consider the likelihood that any incremental speed advantage of RFID technology will be nullified by the fact that border processing – comparing the person to the picture on the PASS Card, and then to the database information – must happen one individual at a time. Thus, the Departments should consider whether the PASS Card would be materially preferable to the new electronic passport.[3]

As required by the DHS appropriations act for fiscal year 2007, DHS and the State Department must work with the National Institute of Standards and Technology (NIST) to ensure that the PASS Card conforms to ISO security standards and best practices relating to the protection of

[3] As discussed below, *see infra* Part IV, CDT believes that there are still privacy and security problems with the new electronic passport.

personal identification documents and the prevention of unauthorized use of information on the card. The Federal Register Notice contains no explicit indication that the GEN-2 RFID-enabled PASS Card can satisfy these Congressional criteria. The Departments must also prevent "mission creep," ensuring that governmental and commercial entities, both domestic and foreign, do not use the PASS Card to identify and track American citizens in unintended ways. In addition, the law requires that a Privacy Impact Assessment be conducted on the privacy risks associated with a given technology choice. While a general WHTI PIA was conducted, CDT urges the Departments to conduct a second PIA that considers the security and privacy risks associated with both long-range (GEN-2) and short-range (ISO 14443) RFID technology. CDT also urges the Departments to conduct in-field testing of both technologies that focuses on security, privacy and operational efficiency. Such testing would provide objective data to inform the development of the PASS Card program, including any related cost-benefit analyses.

In summary, CDT recommends that the State Department find an alternative machine-readable technology for the PASS Card. But if the State Department decides to stay with RFID technology, CDT strongly recommends that long-range GEN-2 technology *not* be used, and that the State Department instead examine adoption of an RFID-enabled short-range PASS Card that is highly secure and protects personal privacy and safety.

II. RADIO FREQUENCY TECHNOLOGY LACKS SECURITY AND THREATENS PRIVACY AND SAFETY

A. An Overview of RFID Technology

RFID is a form of wireless technology. A computer chip attached to an antenna – together referred to as a "tag" – communicates wirelessly with a "reader" or "interrogator" using radio waves. The tag and reader are essentially two-way radios.[4] "Every tag has an identifier that is used to uniquely identify it."[5] The tag communicates its unique ID to the reader (and possibly other information), and the reader is in turn connected to a set of computers "that can store, process, and analyze data acquired from" the tag and reader.[6] Different RFID protocols allow for communication between tag and reader to occur over just a few inches to several feet, or even farther.

The use of radio waves to communicate wirelessly has certain benefits over other wireless technologies: line-of-sight between tag and reader is not required "because radio waves can penetrate many opaque materials," and radio waves allow communication to happen at greater speeds and over greater distances than other wireless technologies.[7] However, these benefits of RFID technology do not appear to be especially relevant to the PASS Card program and, more importantly, these benefits are significantly outweighed by the security and privacy threats posed

[4] National Institute of Standards and Technology, *Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft)*, Special Publication 800-98 (Draft), §2.3 (September 2006) ("NIST Special Publication 800-98") <http://csrc.nist.gov/publications/drafts/800-98/Draft-SP800-98.pdf>.

[5] *Id.* at §2.3.1.1.

[6] *Id.* at §2.2.

[7] *Id.* at §2.1

by long-range RFID technology, in particular.

B. Long-Range RFID Technology Was Designed to Track Products – Not to ID People

The "vicinity read" or long-range RFID technology proposed for the PASS Card refers to the Class-1 Generation-2 protocol developed by EPCglobal, Inc. to track consumer products in the supply chain between manufacturer and retailer, and other inventory. The "GEN-2" tag communicates wirelessly with the reader using radio waves operating at Ultra High Frequency (UHF), in the range of 860 MHz to 960 MHz.[8] UHF tags can be read faster (i.e., more in a given period of time) and from farther distances compared to lower frequency RFID systems.[9]

GEN-2 is an Interrogator-Talks-First (ITF) system[10] in which the reader first "broadcasts a signal that is received by tags in the [reader's] vicinity. Those tags may then be commanded to respond to the [reader] and to continue transactions with the [reader]."[11] The GEN-2 RFID tag is also "passive" meaning that it does not have its own power source – it receives all of its operating energy from the reader.[12] In key ways, therefore, the reader controls the tag. The GEN-2 protocol was adopted as ISO standard 18000-6C.[13]

Long-range RFID technology like that used in the GEN-2 protocol was never meant for human identification. Rather, it was designed for the tracking of *things*. Specifically, UHF RFID was developed to enhance the efficiency of the supply chain – tracking pallets and crates as well as consumer products on retail racks.[14] Because of this intent, security of the UHF RFID system, while important, was not a top priority. A 2001 white paper from MIT's Auto-ID Center, a precursor to EPCglobal, states, "[W]e propose to leave Electronic Product Code simply as a method for naming and identifying objects," and thus "propose to decouple the EPC definition from any security and cryptographic technique."[15]

---

[8] EPCglobal, *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Conformance Requirements Version 1.0.2*, 4 (February 2005) ("EPCglobal GEN-2 Protocol") <http://www.epcglobalinc.org/standards/specs/Class_1_Generation_2_UHF_RFID_Conformance_Requirements_Specification.pdf>.

[9] NIST Special Publication 800-98, *supra* note 4, §2.3.1.3.

[10] EPCglobal GEN-2 Protocol, *supra* note 8, at 4.

[11] NIST Special Publication 800-98, *supra* note 4, §2.3.3.1.

[12] EPCglobal GEN-2 Protocol, *supra* note 8, at 4.

[13] NIST Special Publication 800-98, *supra* note 4, Appendix A.

[14] *See* EPCglobal, *Guidelines on EPC for Consumer Products* <http://www.epcglobalinc.org/public/ppsc_guide/>. EPC stands for "Electronic Product Code," which was intended to replace the bar code-based Universal Product Code (UPC).

[15] David L. Brock, *White Paper: The Electronic Product Code (EPC), A Naming Scheme for Physical Objects*, Auto-ID Center, §4.14 (January 1, 2001) <http://www.rfidjournal.com/whitepapers/download/7>. *See also* ThingMagic, *White Paper: Generation 2 Security*, i (2006) ("ThingMagic White Paper") ("Current levels of data protection provided by the EPCglobal Generation 2 protocol . . . are acceptable for today's limited RFID deployments within the supply chain") <http://www.thingmagic.com/html/pdf/Generation%202%20-%20Security.pdf>.

In a December 2006 report reviewing the use of UHF RFID tags in I-94 forms given to foreign visitors by the US-VISIT program, the Government Accountability Office wrote:

> We and others have raised questions in recent years about the potential privacy risks surrounding the use of RFID technology to track the movement of persons, as *opposed to goods*; the potential for the technology to be subverted for *surveillance* purposes, rather than identification and the potential for "function creep," whereby information collected for one purpose gradually develops other secondary uses, such as has occurred with Social Security numbers.[16]

Because of the insecure-by-design nature of long-range RFID technology, even some in the UHF business have concluded that that "[w]e should not try to force fit security into the existing Generation 2 protocol."[17] In other words, a technology meant to track products cannot be retrofitted with the level of security that is necessary for identifying people.

C. "Unique Reference Number" Can Be Surreptitiously Obtained

The PASS Card Proposed Rule states that the computer chip "would contain only a *unique reference number* [URN] that will serve as a link to information safeguarded in a secure database managed by" Customs and Border Protection.[18] This is often called a "pointer system" because the URN (i.e., the tag's unique ID) "points" to personally identifiable information (PII) in a back-end database. The State Department and DHS assert that a pointer system is preferable to having PII stored on the PASS Card itself.[19] However, the URN, if obtained by unauthorized persons, can be linked to PII.[20] And even if the unique reference number is not discovered or does not lead to PII, a person carrying an RFID-enabled card is still at risk of being tracked.

The tag and reader segment of an RFID system – the "front-end" – has the weakest security; it is

---

[16] Government Accountability Office, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248, Appendix VI: Actions Taken by US-VISIT Program Office to Mitigate Privacy Risks Associated With RFID at Land POEs, 81 (December 2006) ("GAO-07-248") (emphasis added) <http://www.gao.gov/new.items/d07248.pdf>.

[17] ThingMagic White Paper, *supra* note 15, at 13.

[18] PASS Card Proposed Rule, *supra* note 1, at 60930 (emphasis added).

[19] *See id.* (the PASS Card "will only store and transmit a unique reference number and no personal or biographic information"). *See also* Department of Homeland Security, *Fact Sheet: Western Hemisphere Travel Initiative (WHTI) Passport Card Technology Choice: Vicinity RFID* (October 17, 2006) ("DHS WHTI Fact Sheet") ("Through the passport card design, personal privacy would be protected through multiple layers of security . . . No personal information would be transmitted or stored on the vicinity RFID-enabled card. The technology will transmit only a number between the card and the reader which will be matched against a DHS database") <http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm>.

[20] There is the possibility that a person could hack into the back-end database and use the URN to access PII. However, as discussed *infra* Part III.D. with regard to "mission creep," a greater concern is that the URN will be used as a unique identifier and link to a vast amount of personal information gathered by other means (e.g., point-of-sale, sensor networks).

"the Achilles' heel of RFID systems."[21] Generally, a tag's unique ID can be obtained in two ways: 1) by initiating a fake transaction with the RFID tag using a rogue reader, sometimes called *skimming*, or 2) by *eavesdropping* on an authorized transaction using a receiver.[22] The "security" features that are part of the GEN-2 protocol do not sufficiently guard against skimming or eavesdropping.[23] DHS asserts that it "is taking steps to ensure that [the URN] cannot be intercepted during transmission to an authorized reader at a port of entry"[24], yet the State Department's Proposed Rule does not state how eavesdropping will be prevented. In addition, generally speaking, "RFID tags indiscriminately respond to RFID interrogation at the proper frequency and cannot differentiate between a rogue and authorized reader."[25] If this is the case with the RFID system proposed for the PASS Card – and there is nothing in the Proposed Rule to indicate otherwise – then any person with a UHF reader, whether a CBP officer or not, could scan for PASS Cards in people's wallets and "skim" their unique reference numbers.

1. Tag Password is Discoverable

The GEN-2 protocol provides for an *optional* 32-bit password (as opposed to the 8-bit password in the GEN-1 UHF tag) that controls access to the tag's unique ID.[26] The State Department has not said whether a password will be part of the PASS Card's RFID chip.[27] Regardless, the password can still be discovered with relative ease by analyzing changes in a passive tag's power output, a process known as "power analysis attack."[28] In fact, the 8-bit password on a GEN-1 tag was cracked in about one minute by power analysis attack.[29] Furthermore, while a password can mitigate against a rogue reader obtaining the URN by skimming the RFID tag, the password can easily also be obtained by *eavesdropping* on a legitimate transaction, assuming the reader sends the password to the tag in clear text.[30]

An additional and significant security concern is that if the same password is used for all RFID

---

[21] ThingMagic White Paper, *supra* note 15, at 5.

[22] *See id.* at 6. *See also* Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security, *The Use of RFID for Human Identity Verification*, Report No. 2006-02 ("DHS Privacy Advisory Committee RFID Report") §VI.C. (December 6, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf>.

[23] *See, e.g.*, ThingMagic White Paper, *supra* note 15, at 7.

[24] DHS WHTI Fact Sheet, *supra* note 19.

[25] US-VISIT RFID White Paper, *supra* note 2, §2.2.3.

[26] EPCglobal GEN-2 Protocol, *supra* note 8, at 21.

[27] While GEN-2 tags have a longer password than GEN-1 tags, the GEN-2 protocol was designed to enhance interoperability between tags and readers, thereby increasing the number of readers that can read the tags. *See* EPCglobal, *RFID Implementation Cookbook*, Chapter 2.4 <http://www.epcglobalinc.org/what/cookbook/chapter2/>.

[28] NIST Special Publication 800-98, *supra* note 4, §5.3.1.1 and n.51.

[29] Mary Catherine O'Connor, "EPC Tags Subject to Phone Attacks," *RFID Journal* (February 24, 2006) <http://www.rfidjournal.com/article/articleprint/2167/-1/1>.

[30] NIST Special Publication 800-98, *supra* note 4, §5.3.2.4.

tags, then a misfeasor who discovers the password can use it to discover the URNs for *all* PASS Card holders.[31] It is technically possible to create a unique password for each PASS Card, but the costs in key management far outweigh the savings of using the cheaper GEN-2 RFID tag.[32] As stated above, it is not technologically appropriate to "try to force fit security into the existing Generation 2 protocol."[33] The Proposed Rule gives no indication whether the State Department considered these issues.

2. Cover Coding Is Not Encryption

The GEN-2 protocol also calls for "cover coding," which is a way of masking the URN or the password sent to the tag by the reader.[34] Also, the Proposed Rule states that the PASS Card will "utilize the international standard for Machine Readable Zone (MRZ) encryption."[35] However, CDT is concerned that neither of these are true encryption as the GEN-2 RFID tag cannot – by design – support encryption.[36]

In any event, cover coding is susceptible to eavesdropping: the cover coding "key" can be obtained by intercepting the tag's response to the reader, which can then be used to decipher the password and ultimately uncover the URN. Additionally, even if the password or URN are never obtained, the cover coding key – if it remains constant for a given RFID tag – itself can act like a URN: a unique identifier for that particular PASS Card and hence that particular person.[37]

3. Long Read Range Increases the Risk of Skimming and Eavesdropping

The lack of meaningful security features inherent in the GEN-2 protocol is exacerbated by the long read range of the system. A GEN-2 RFID tag has a "nominal operating range" of 15-20 feet.[38] Eavesdropping ranges, on the other hand, "can be significantly greater than the nominal operating ranges listed in product literature" – for example, eavesdropping on reader-to-tag communication (e.g., obtaining the password) can sometimes occur, under ideal conditions, from *kilometers* away.[39] Thus someone can be can be very far away from the GEN-2 RFID tag or its authorized reader and still successfully compromise a PASS Card.

---

[31] *Id.* at §5.3.1.1.

[32] *See* US-VISIT RFID White Paper, *supra* note 2, §2.3.5.

[33] ThingMagic White Paper, *supra* note 15, at 13.

[34] *See id.* at 10. *See also* NIST Special Publication 800-98, *supra* note 4, §5.3.2.4, Appendix A.2.

[35] PASS Card Proposed Rule, *supra* note 1, at 60930.

[36] *See* NIST Special Publication 800-98, *supra* note 4, §5.3.1.3.

[37] *See* DHS Privacy Advisory Committee RFID Report, *supra* note 22, §VI.C. (stating that encryption "is not a complete solution" because "[t]hough indecipherable itself, the encrypted information can act as an identifier if it remains the same each time the card is skimmed, just as a person might be known by a nickname"). *See also* US-VISIT RFID White Paper, *supra* note 2, §3.3.2.

[38] NIST Special Publication 800-98, *supra* note 4, §2.3.1.3 (15 feet). PASS Card Proposed Rule, *supra* note 1, at 60930 (20 feet).

[39] NIST Special Publication 800-98, *supra* note 4, §2.3.3.3.

4. Protective Sleeve Places the Burden on the PASS Card Holder

The Proposed Rule states that the PASS Card will be issued "with a thin protective sleeve, which is designed to protect the card from unauthorized access. The card could be stored in the sleeve and removed only when needed."[40] However, this improperly places the burden of ensuring personal privacy and security on the PASS Card holder.[41] A government-issued document as important as the PASS card – needed to prove identity and citizenship to reenter one's own country – should not be so devoid of security features that a person's only hope is to keep the card in the protective sleeve. At the least, education will be an important factor here. Many people using RFID-enabled automated toll collectors, for example, throw away the Mylar bag the transponder comes in, thinking that the bag is simply packaging. But even the best education will not provide strong security for individuals because the protective sleeve does not prevent eavesdropping on an authorized transaction at the border – when the PASS card must be removed from the sleeve.

III. THREATS TO A PASS CARD HOLDER'S PRIVACY AND SAFETY

The State Department and DHS failed to conduct a Privacy Impact Assessment (PIA) on the PASS Card and the use of RFID technology. A PIA is supposed to identify all possible risks associated with a technology used in the collection, maintenance or dissemination of personal information. A PIA must identify possible privacy risks associated with the use of the technology, the likelihood of those risks, and the existence of measures that can mitigate or eliminate the risks.[42]

Here we identify four immediately apparent risks that should be considered by the Departments, but we emphasize that a PIA should address the full range of risks associated with the creation of the PASS Card and the use of RFID technology.

A. "Unique Reference Number" Might Reveal Personal Information

A PASS Card holder's data privacy can be significantly compromised once the unique reference number is known. The State Department and DHS assert that using a URN to point to a database is preferable to having personally identifiable information (PII) stored on the PASS Card itself.[43] However, the State Department has not clarified whether the URN itself will encode PII.

Every RFID tag has a unique ID[44] that can be created in two ways: it can have a "standard

---

[40] PASS Card Proposed Rule, *supra* note 1, at 60931.

[41] *See* US-VISIT RFID White Paper, *supra* note 2, §2.3.3 (stating that the Faraday Cage "can be used to shield a tag from unwanted eavesdropping, but requires owner compliance for use"). *See also* DHS Privacy Advisory Committee RFID Report, *supra* note 22, §VI.C. (questioning the effectiveness of a wrapper or sleeve for an RFID-enabled ID card).

[42] *See infra* Part V for a more detailed discussion of the Privacy Impact Assessment.

[43] *See supra* note 19.

[44] NIST Special Publication 800-98, *supra* note 4, §2.3.1.1.

structure, with certain groups of bits representing particular fields," or it can be a number that reveals nothing about the tagged item – such a number can be random or serialized.[45] The State Department proposes to follow the GEN-2 RFID protocol, which creates a tag's unique ID by following a standardized Electronic Product Code format.[46] This poses a significant privacy problem. If the URN "is generated via an algorithm that uses personally identifiable information as its basis, knowledge of the number generation algorithm may permit 'decoding' of the tag number and provide information about the individual to whom the tag was assigned."[47]

CDT urges the State Department to clarify how the URN will be created – in other words, whether the URN will encode any personally identifiable information.[48]

B. The URN Can Be Used to Track the PASS Card Holder

If a PASS Card's unique reference number is captured, that number – which is permanently associated with the PASS Card – can be used to track the card holder. Once a URN is associated with a particular person, anyone with a UHF reader or a network of UHF readers can use it to track the movements of the PASS Card holder. People carrying RFID-enabled documents "may not always know when they are being identified and to whom unless people begin carrying radio frequency detectors or purses and wallets that are impermeable to radio frequencies."[49]

C. Location Privacy Risks When the URN Is Not Known

Even if a tag's unique ID is not known, a person with an RFID-enabled document can still be tracked. Any number such as a cover coding key or password meant to mask information on an RFID tag, if it is permanently associated with the tag, can itself be used as a unique identifier to track the PASS Card holder.[50]

Additionally, even if no unique identifier is associated with a particular PASS Card and thus a particular person, the RFID tag can act like a beacon announcing its presence. An appropriately configured UHF reader can emit a signal and sufficient power that commands every tag in the area to respond. Even if no valuable information can be gleaned from a tag's return signal, the mere detection of RFID activity can announce that the person is likely an American citizen – and

---

[45] *Id.*

[46] *Id.* at §5.2.6.

[47] US-VISIT RFID White Paper, *supra* note 2, §3.3.1.

[48] *See id.* at §3.2, §3.3.1.

[49] DHS Privacy Advisory Committee RFID Report, *supra* note 22, §VI.B.

[50] *See id.* at §VI.C. (stating that encryption "is not a complete solution" because "[t]hough indecipherable itself, the encrypted information can act as an identifier if it remains the same each time the card is skimmed, just as a person might be known by a nickname"). *See also* US-VISIT RFID White Paper, *supra* note 2, §3.4 ("even if the tag number is encrypted, location privacy may be compromised if the tag responds with the same encrypted response every time it is read").

the perfect target for a crime or terrorism.[51] And this can happen "over much greater distances than eavesdropping."[52]

D. Preventing "Mission Creep" by Government and Business

The general WHTI Privacy Impact Assessment discusses the possible "misuse" of border crossing data and states that access to such data within the government will be strictly controlled.[53] However, because the PIA does not concern the PASS Card and the use of GEN-2 RFID technology specifically, the PIA fails to address the threat to personal privacy if the U.S. government, state or local governments, law enforcement agencies, foreign governments or entities, or even businesses were to use the PASS Card for other purposes beyond the intended one.[54]

For example, if the PASS Card were used as identification in a non-border transaction, a business could use the URN as an identifier and permanently link it to the person's name and any other personal information gathered at the point-of-sale. Similarly, RFID-enabled ID documents like the PASS Card may inspire the broader development of "sensor networks" by government or business, which can track people and link location and travel data to other PII.[55] The concerns associated with PASS Card "mission creep" are not unlike those associated with the now ubiquitous use of Social Security Numbers, an identifier created for one purpose and now used for many.[56]

The State Department must explain whether and how it will be able to prevent other government or law enforcement agencies, foreign governments and entities, and businesses from using the RFID-enabled PASS Card to identify and track American citizens outside the border crossing context.

---

[51] *See* NIST Special Publication 800-98, *supra* note 4, §2.3.3.3. *See also* US-VISIT RFID White Paper, *supra* note 2, §3.3.1.

[52] NIST Special Publication 800-98, *supra* note 4, §2.3.3.3.

[53] Department of Homeland Security, *Privacy Impact Statement for the Western Hemisphere Travel Initiative (WHTI)* §1.1 (August 11, 2006) ("WHTI PIA") <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_whti.pdf>.

[54] US-VISIT RFID White Paper, *supra* note 2, §3.3.2.

[55] *See, e.g.*, Pamela Samuelson, Director, Berkeley Center for Law & Technology, University of California, Boalt Hall School of Law, "Sensor Networks & Privacy," presentation given at *Securing Privacy Conference*, Stanford University (March 13, 2004) <http://www.ischool.berkeley.edu/~pam/papers.html>. *See also* Sensor Network Consortium (SNC), Center for Information & Systems Engineering, Boston University <http://www.bu.edu/systems/industry/consortium/index.html>.

[56] *See* GAO-07-248, *supra* note 16, at 81. *See also* Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly Media, 20, 32 (2000).

IV. THE PASS CARD PROPOSED RULE FAILS TO ADDRESS THE NIST SECURITY CERTIFICATION AND BEST PRACTICES CONGRESSIONAL REQUIREMENTS

As far as CDT can determine, the State Department has picked RFID for the PASS Card without review by the National Institute of Standards and Technology (NIST), in violation of the recent congressional mandate. In the DHS appropriations act for fiscal year 2007, Congress amended §7209(b)(1) of the Intelligence Reform & Terrorism Act of 2004, requiring the State Department and DHS to receive NIST certification that the PASS Card "meets or exceeds International Organization for Standardization (ISO) security standards and meets or exceeds best available practices for protection of personal identification documents," including "the best available practices to prevent the unauthorized use of information on the card."[57]

The PASS Card Proposed Rule makes no mention of NIST certification, security standards or best practices. CDT agrees with Senator Patrick Leahy (D-Vermont), chief sponsor of the NIST amendment, who noted with frustration after the Proposed Rule was published: "Earlier this month Congress prescribed repairs to fix PASS Card's worst problems, but so far these agencies have blithely ignored the help . . . . Though our amendment has been moving toward enactment for most of this year, the Administration has failed to incorporate most of these improvements into their plan."[58]

A. ISO 14443 Is Not a "Security Standard"

An obvious question is, What did Congress mean when it required agencies to adhere to "ISO security standards" and "best practices"? The Senate version of the 2007 DHS appropriations act would have required NIST to certify that the PASS Card "architecture meets . . . ISO 14443 security standards, or justifies a deviation from such a standard."[59] However, Congress removed any mention of ISO 14443 from the final version of the NIST provision. The enacted law also provides, "That to facilitate efficient cross-border travel, the Departments of Homeland Security and State shall, to the maximum extent possible, develop an architecture that is compatible with information technology systems and infrastructure used by United States Customs and Border Protection."[60]

The State Department notes that the ISO 14443 standard is currently being used for the new

---

[57] Department of Homeland Security Appropriations Act of 2007 [H.R. 5441] Pub. L. No. 109-295, § 546, 120 Stat. 1355 (Oct. 4, 2006) ("DHS Act FY2007"), *amending* §7209(b)(1) of the Intelligence Reform & Terrorism Prevention Act of 2004 [S. 2845] Pub. L. 108-458, 118 STAT. 3823 (December 17, 2004).

[58] Comments Of Sen. Patrick Leahy (D-Vt.) (Chief Sponsor Of The Leahy-Stevens Amendment) On The State Department's Proposed Rule, Issued Tuesday, To Implement The PASS Card Border ID System, Part Of The Western Hemisphere Travel Initiative (WHTI) Tuesday, Oct. 17, 2006 ("Leahy Comments") <http://leahy.senate.gov/press/200610/101706a.html>.

[59] Department of Homeland Security Appropriations Act of 2007, Engrossed Amendment as Agreed to by Senate [H.R. 5441 EAS] 68-69 (July 13, 2006).

[60] *See* DHS Act FY2007, *supra* note 57.

electronic passport.[61] ISO 14443 is a protocol for wireless communication between a tag and reader using radio waves operating at 13.56 MHz, in the High Frequency (HF) – not UHF – range.[62] Because of this lower frequency, the nominal operating read range for RFID tags conforming to ISO 14443 is 10 centimeters or approximately four inches.[63] ISO 14443 is not applicable to the "vicinity read" technology chosen by the State Department and, more importantly, is not a security standard. ISO 14443 "does not currently address a means to achieve a common framework for data integrity, authentication, and general security mechanisms . . . Most existing ISO 14443-based card technology implantations center on proprietary security schemes."[64]

While the optimal read range for ISO 14443 devices is 10 centimeters, the rogue scanning range is at least 50 centimeters (cm), or five times the standard's nominal operating range.[65] Thus even the shorter read range associated with ISO 14443 may pose security concerns. Smart cards, which use ISO 14443 technology, often have enhanced security features, such as encryption. However, such security features are generally added by the manufacturer, not by requirement of the ISO 14443 protocol. Furthermore, there is no indication in the Proposed Rule that the State Department has considered what security features it would add if it were to adopt short-range RFID technology for the PASS Card. Clearly, this is an issue that would require further attention if the State Department were to pursue "proximity read" RFID technology for the PASS Card, recognizing that, as a practical matter, security must be carefully designed and implemented. For example, in August 2006, a German computer security expert explained at a hacker convention that he accessed personal information on an allegedly secure electronic passport issued by the German government.[66]

---

[61] PASS Card Proposed Rule, *supra* note 1, at 60930.

[62] NIST Special Publication 800-98, *supra* note 4, Appendix A.1.

[63] *Id.* at §2.3.1.3 n.7.

[64] National Institute of Standards and Technology, *Card Technology Developments and Gap Analysis*, Interagency Report 7056, §4.4.2, §2.2.3 (March 2004) <http://csrc.nist.gov/publications/nistir/nistir-7056.pdf>. *See also* On Track Innovations, Ltd., *White Paper: ISO 14443: An Introduction to the Contactless Standard for Smart Cards and Its Relevance to Customers*, 9 <http://www.otiglobal.com/objects/ISO%2014443%20WP%204.11.pdf>.

[65] NIST Special Publication 800-98, *supra* note 4, §2.3.3.3.

[66] *See* Kim Zetter, "Hackers Clone E-Passports," *Wired News* (August 3, 2006) <http://www.wired.com/news/technology/0,71521-0.html>. *But see* Mary Catherine O'Connor, "Industry Group Says E-Passport Clone Poses Little Risk," *RFID Journal* (August 9, 2006) <http://www.rfidjournal.com/article/articleview/2559/1/1/>. Smart card manufacturers state that e-passports are "secure," emphasizing that even if cloned, data on the chip is very difficult to alter and, thus, a visual inspection by a border agent comparing the data on the chip with the person presenting the passport will reveal that the passport is fake. However, while tampering with personal information might be difficult, the fact that personal information, even if encrypted, can be gleaned from an electronic passport greatly threatens the citizen's privacy and safety. *See, e.g.*, Annalee Newitz, "The RFID Hacking Underground," *Wired Magazine* (May 2006) <http://www.wired.com/wired/archive/14.05/rfid.html?pg=3&topic=rfid&topic_set=>. An objective, detailed studying clarifying the privacy and security risks associated with both long-range and short-range RFID technology, including the use of short-range RFID technology in e-passports and smart cards, would greatly inform the PASS Card program.

It is important to note that "[t]he major laws, executive orders, and programs under which RFID is being considered or used are either permissive as to technology or not legally binding on the U.S. government."[67] Thus, should the State Department move forward with creating a PASS Card, it is statutorily free to use something other than RFID technology to fulfill the program's mission – so long as the technology meets or exceeds ISO security standards and best practices for protection of personal identification documents. Furthermore, the compatibility clause is permissive, stating only that the PASS Card be interoperable with other initiatives "to the maximum extent possible." Therefore Congress' encouragement to make the PASS Card compatible with other border technologies does not trump Congress' requirement that the PASS Card system be secure.

B. Several "Best Practices" Sources Should Be Consulted

The State Department can look to several sources of best practices relating to the protection of personal identification documents and the prevention of unauthorized use of information on the PASS Card. A starting point is the draft DHS Privacy Advisory Committee RFID Report, which identifies a technology-neutral set of best practices: Notice, Open Standards, Choice and Control (Consent), Securing Readers and Data, Avoid Function Creep, and Education Campaign.[68]

There are other sources of best practices to ensure privacy and security. CDT facilitated the development of Authentication Privacy Principles,[69] as well as best practices for the use of RFID technology in the consumer context.[70] NIST recommends 17 "privacy control families" and also endorses the data privacy guidelines developed by the Organisation for Economic Co-operation and Development (OECD).[71] The CDT website references other sources of "fair information practices."[72] The State Department should consider these and other best practices sources to guide the development of the PASS Card system and ensure the maximum level of data security and personal privacy and safety.

---

[67] DHS Privacy Advisory Committee RFID Report, *supra* note 22, §IV.

[68] *Id.* at §VII.B.

[69] Center for Democracy & Technology, *Authentication Privacy Principles Working Group* (May 13, 2003) <http://www.cdt.org/privacy/authentication/030513interim.shtml>.

[70] Center for Democracy & Technology, *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology* (May 1, 2006) <http://www.cdt.org/privacy/20060501rfid-best-practices.php>.

[71] NIST Special Publication 800-98, *supra* note 4, §6.1, §6.3. *See also OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) <http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html>.

[72] Center for Democracy & Technology, *Privacy Basics: Fair Information Practices* <http://www.cdt.org/privacy/guide/basic/fips.html>.

V. A PRIVACY IMPACT ASSESSMENT SHOULD BE CONDUCTED FOR RFID TECHNOLOGY

A. The Law Requires That a Privacy Impact Assessment Be Conducted for the PASS Card

Not only has the State Department failed to work with NIST, it has also failed to conduct an adequate Privacy Impact Assessment for the PASS Card. A general WHTI Privacy Impact Assessment was conducted by DHS, but it focuses on the collection of passport information and travel histories of persons previously exempted from presenting a passport or other proof of identity and citizenship at U.S. land and sea borders – namely, American citizens and non-immigrant aliens from Canada, Mexico and Bermuda.[73]

The general WHTI PIA does not specifically address the privacy and security implications of the PASS Card and the use of RFID technology. It simply states, "Information collected from travelers under WHTI . . . will be collected by running the machine readable zone (MRZ) of the passport through a scanner-like reader or through the use of *other technology like RFID chips* in documents like the ePassport so as to minimize human error in inputting information into the system."[74] No further technological analysis was conducted.

A PIA that specifically considers the privacy and security threats of using RFID tags in the PASS Card would be immensely helpful and is in fact required by law. The E-Government Act of 2002 requires that an agency conduct a Privacy Impact Assessment "before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form."[75] "Identifiable form" refers to "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[76] The Homeland Security Act of 2002 requires that DHS, specifically, conduct PIAs and that the Department use technologies that "sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."[77] These laws clearly apply to the use of RFID technology in the PASS Card.

Similarly, the DHS PIA guide states that a PIA should be conducted when an agency is "developing or procuring any new technologies or systems that handle or collect personal information."[78] The guide explains, "Examples of technology with privacy implications could include systems utilizing *radio frequency identification devices (RFID)*, biometric scans, data

---

[73] WHTI PIA, *supra* note 53, §1.1.

[74] *Id.* at §2.3.

[75] E-Government Act of 2002 [H.R. 2458] Pub. L. 107-347, §208(b)(1)(A), 116 STAT. 2921 (December 17, 2002).

[76] *Id.* at §208(d).

[77] Homeland Security Act of 2002 [H.R. 5005] Pub. L. 107-296, §222, 116 STAT. 2155 (November 25, 2002).

[78] Department of Homeland Security Privacy Office, *Privacy Impact Assessments: Official Guidance*, 12 (March 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_march_v5.pdf>.

mining, or geospatial tracking."[79]

Regarding US-VISIT's inclusion of long-range RFID tags in I-94 forms, the Government Accountability Office stated that "a privacy impact statement should be conducted before an agency develops or procures an information technology system, such as the proposed RFID system, which collects, maintains, or disseminates information about an individual – in this case, numeric information that may be linked to biographic information contained within databases."[80] The GAO also stated in an earlier report that "the privacy impact assessments required by the E-Government Act of 2002 provide an existing framework for agencies to follow in assessing the impact on privacy when implementing RFID technology."[81]

Thus it is clear that the general WHTI Privacy Impact Assessment is insufficient as it does not cover the proposed development of the PASS Card. CDT urges the creation of another PIA that specifically considers the threats to personal privacy and safety of using an RFID tag – whether long-range or short-range – in the PASS Card.[82]

B. Testing of RFID Technology Would Inform the Privacy Impact Assessment

Testing should be conducted to more objectively assess the privacy and security risks of using both long-range and short-range RFID technology. Testing would inform a PIA and might lead to the selection of a more secure wireless technology. In fact, Senator Leahy, chief sponsor of the NIST amendment, lamented, "Without even testing the technology for use as a passport or personal ID, they have chosen a weaker security standard that would make our borders less secure and that would risk the personal information of millions of Americans."[83] Testing is important because, as tests of the use of long-range RFID tags in the I-94 forms has shown, RFID has some serious security – and even reliability – problems.[84]

---

[79] *Id.* at 11 (emphasis added).

[80] GAO-07-248, *supra* note 16, at 81, *citing* Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB M-03-22 (September 26, 2003) <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

[81] Government Accountability Office, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551, 3 (May 2005) < http://www.gao.gov/new.items/d05551.pdf>.

[82] In the PIA related to the collection of personal information from e-passports issued by other countries, DHS states, "[I]n the case of U.S. issued e-Passports, the Department of State (DOS) is assessing the risks presented by the passports themselves and determining how best to mitigate them." Department of Homeland Security, *Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, Authentication of e-Passports* (August 18, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_epassport.pdf>. We find it disturbing that the State Department is apparently still in the process of determining the privacy risks of using RFID technology in e-passports – even though the new passports are already being issued. *See* Department of State, Office of the Spokesman, "Department of State Begins Issuing Electronic Passports to the Public," Media Note (August 14, 2006) <http://www.state.gov/r/pa/prs/ps/2006/70433.htm>. We stress that the State Department must determine the privacy risks of using RFID technology in the PASS Card *before* the cards are issued to American citizens.

[83] Leahy Comments, *supra* note 58.

[84] *See* GAO-07-248, *supra* note 16, Appendix VI: Actions Taken by US-VISIT Program Office to Mitigate

VI. THE POLICY JUSTIFICATIONS FOR THE LONG-RANGE RFID TECHNOLOGY CHOICE ARE UNPERSUASIVE

The State Department's justifications for choosing to create the PASS Card, and incorporate long-range RFID technology into it, are unpersuasive, and – more importantly – do not outweigh the security and privacy threats associated with GEN-2 RFID technology.

It is important to note that the Intelligence Reform & Terrorism Act of 2004 did not require the development of the PASS Card and, furthermore, was "silent on whether [the passport or similar document] should be read electronically."[85] It simply "require[d] a passport or other document, or combination of documents [that] sufficient[ly] [] denote identity and citizenship [] for all travel into the United States by United States citizens."[86] It was the NIST amendment in the 2007 DHS appropriations act that first mentioned a "passport card" and "technology"[87] – because at that point DHS and the State Department were actively planning the PASS Card and the integration of an RFID chip. Yet even so, as discussed above, the NIST amendment does not mention or require the use of RFID technology in the PASS Card.

A. "Pre-Positioning" Using Long-Range RFID Technology Will Not Increase Efficiency

The State Department and DHS believe that the use of long-range RFID technology in the PASS Card will increase efficiency at the border. The PASS Card Proposed Rule states that "the use of vicinity technology would provide information to border security personnel further in advance of a traveler's arrival at an inspection booth."[88] In other words, the long read range of the GEN-2 RFID tag would enable retrieval of personal information from the back-end database before a person reaches the inspection agent. DHS similarly stated: "Multiple cards can be read at a distance and simultaneously with vicinity RFID technology, allowing an entire car full of people to be processed at once."[89]

However, this is at odds with the border security benefits of having an electronic ID card in the first place. One apparent purpose of an electronic ID card is to ensure that the face of the card has not been tampered with and that the person seeking entry is in fact an American citizen. A CBP officer must look at the person, look at the card, and look at the information contained in the database – and confirm that all three match. The PASS Card Proposed Rule admits that the

---

Privacy Risks Associated with RFID at Land POEs; Appendix VII: US-VISIT Test of Radio Frequency Identification (RFID) Readers Upon Exit and Re-entry at Selected Land POEs.

[85] Government Accountability Office, *Observations on Efforts to Implement the Western Hemisphere Travel Initiative on the U.S. Border with Canada*, GAO-06-741R, 4 n.8 (May 25, 2006) <http://www.gao.gov/new.items/d06741r.pdf>.

[86] Intelligence Reform & Terrorism Act of 2004 [S. 2845] Pub. L. 108-458, §7209(b)(1), 118 STAT. 3823 (December 17, 2004).

[87] Department of Homeland Security Appropriations Act of 2007 [H.R. 5441] Pub. L. No. 109-295, § 546, 120 Stat. 1355 (Oct. 4, 2006).

[88] PASS Card Proposed Rule, *supra* note 1, at 60930.

[89] DHS WHTI Fact Sheet, *supra* note 19.

CBP officer would still have to "compare the citizen presenting him or herself for entry into the U.S. with the original issuance record to ensure that it is the same person."[90] But comparison of the person, the card, and the database information must happen *one individual at a time*. Thus the "pre-positioning" of database information when a person is 20 feet away – or the simultaneous pre-positioning of data on multiple people at this greater distance – is a benefit of long-range RFID technology irrelevant in the border crossing context.[91]

B. Speed of RFID Communication Is of Questionable Benefit

As discussed above, in addition to a longer read range, RFID communication has other advantages over other types of wireless technology: communication between tag and reader happens faster, and line-of-sight between tag and reader is not necessary. The State Department asserts that RFID technology "would allow passengers approaching a land crossing in vehicles 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."[92] Similarly, DHS asserts that "[t]he speed of vicinity RFID will allow CBP officers to quickly read the identification of all travelers carrying passport cards, allowing DHS to perform terrorist watch list checks."[93]

However, the asserted increase in efficiency due to the faster speed of wireless radio communication – whether long-range or short-range – is questionable, especially given the need, mentioned above, to individually compare the card with the card holder. CDT urges the State Department and DHS to undertake objective testing to determine whether the use of RFID technology would create a material increase in processing time at the border over other machine-readable technologies. Only after any benefits have been reliably quantified is it necessary to reach the question of whether they outweigh the privacy and security concerns we have raised.

C. The Benefits of Interoperability with Other Systems Designed for Other Uses Are Questionable

The State Department has chosen GEN-2 RFID technology for the PASS Card "to leverage existing technologies, including programs such as CBP's Trusted Traveler programs NEXUS, FAST, and SENTRI and use of the electronic I-94 . . . . The selection of vicinity read technology for the passport card was made in an effort to ensure a seamless operational environment with

---

[90] PASS Card Proposed Rule, *supra* note 1, at 60930 .

[91] *See* DHS Privacy Advisory Committee RFID Report, *supra* note 22, §V.B. ("Transmitting information via radio in advance can [] allow information to be 'pre-positioned' before an individual approaches an entrance or checkpoint," but "the verifier must still review authorizing information and compare the identifiers from the card with the bearer in order to ensure that the RFID-enabled card is being carried by the person with whom it is associated").

[92] PASS Card Proposed Rule, *supra* note 1, at 60930.

[93] DHS WHTI Fact Sheet, *supra* note 19. While not central to the PASS Card Proposed Rule and these comments, we wanted to flag the fact that the federal government apparently places American citizens on "terrorist watch lists" and will apprehend them at land borders when they try to renter their own country using the PASS Card.

DHS."[94] However, the State Department failed in its Proposed Rule to explain how the PASS Card system and the other systems will in fact be interoperable and failed to identify, let alone quantify, any concrete benefits of interoperability. As discussed above in relation to the NIST amendment, compatibility of technologies may be desired but is not required, and certainly cannot trump serious security and privacy concerns.

D. Cheaper Cost is Not a Reason to Choose an Insecure Technology for Border Security

The PASS Card is meant to be a low-cost alternative to the passport book (including the new electronic passport) for U.S. citizens who frequently cross the border by land or sea.[95] The Proposed Rule states that the proposed fees for the PASS Card take into account "the direct costs of producing passport cards, the card stock, technology, adjudicating the application, printing the biographic information on the card, and priority mail return for the card."[96] While GEN-2 RFID technology is relatively inexpensive[97], its cheaper cost does not outweigh the significant threats to personal privacy and safety posed by the standard. CDT urges the Department to conduct a detailed cost-benefit analysis that weighs the potential gains of using GEN-2 against the risks of using this inherently insecure standard.

If the State Department were to adopt a highly-secure machine-readable technology for the PASS Card, or even the short-range RFID technology used in smart cards, the cost of the PASS Card would likely be much closer to that of the passport book. Thus CDT urges the State Department to determine whether an appropriately secure PASS Card would be materially different from the passport book (including the e-passport) in terms of function and cost.[98]

---

[94] PASS Card Proposed Rule, *supra* note 1, at 60930-60931.

[95] PASS Card Proposed Rule, *supra* note 1, at 60929 ("The passport card is intended as a lower cost means of establishing identity and nationality for American citizens in two limited situations – for citizens crossing U.S. land borders and traveling by sea between the U.S., Canada, Mexico, the Caribbean, or Bermuda").

[96] PASS Card Proposed Rule, *supra* note 1, at 60931.

[97] *See, e.g.*, NIST Special Publication 800-98, *supra* note 4, §5.3.1.3 ("Tags that support onboard encryption currently are more costly than those that do not . . . most low-cost passive tags do not have enough logic gates to perform complex encryption algorithms").

[98] People who are motivated to buy the PASS Card because of its lower price may later find that they need a bona fide passport for other international travel. Thus they will have spent *even more* money buying two ID documents for international travel.

VII. CONCLUSION

In summary, CDT recommends that the State Department:

- Determine whether the PASS Card, if security and privacy concerns are addressed, would be materially different from the new electronic passport, and thus whether the PASS Card program is necessary;
- If moving forward with the PASS Card program, examine alternatives and choose a technology other than RFID as the machine-readable technology for the PASS Card;
- Reject long-range GEN-2 RFID technology because it is inherently insecure and would pose significant privacy and safety risks to the PASS Card holder;
- If short-range RFID technology is considered for the PASS Card, determine how data and location privacy risks can be minimized;
- Consult with NIST in order to obtain security and "best practices" certification for the machine-readable technology;
- Develop measures to prevent "mission creep" (i.e., use of the PASS Card in unintended ways);
- Conduct in-field testing of the machine-readable technology that objectively looks at privacy, security, and any other possible benefits such as increased efficiency;
- Conduct detailed cost-benefit analyses of proposed machine-readable technologies, informed by the field testing;
- Conduct a Privacy Impact Assessment for both long-range and short-range RFID technology;
- If RFID technology is still adopted, develop a plan for an education campaign that informs PASS Card holders of how they can protect their privacy, such as by using a protective sleeve.

We look forward to working with the Departments of State and Homeland Security, Congress, the technology industry and all stakeholders to develop a sound mechanism for protecting America's borders that does not entail unacceptable risk to personal privacy and security.

Sincerely,

Sophia Cope
Staff Attorney/Ron Plesser Fellow
Center for Democracy & Technology