Remarks by
Frank E. Moss
Deputy assistant secretary
For passport services
U.S. Department of State
To the
Smart Card Alliance
Crystal City, Virginia
April 18, 2006

Good afteroon. I want to begin my remarks by thanking randy vanderhoof for inviting me to meet with you to discuss the department of state's passport initiatives. I will try to be brief since I know that is late afternoon, you still have another speaker and many of you are probably thinking about the social and networking opportunities that await you this evening.

Now, in the interest of full disclosure, I must begin my remarks with the following important announcements. These include:

1. I was labeled by at least one person filing comments on our e-passport federal rulemaking process as the anti-Christ. The individual who made the comment went on to call anyone who cooperated with me in this effort a minion of the anti-Christ whose name will also be removed from the book of life.
2. The organization citizens against government waste (cawg.org) has awarded me the title of "porker of the month for February 2006" for my role in the e-passport program

If anyone wishes to leave now, I won't be offended!

I also have one request I would like to make. If you have a question while I deliver my remarks, put up your hand and "fire away".

Let me begin my substantive remarks by providing a brief summary of us. Passport operations. These numbers, I think, are important to understand why we made some of the decisions that we did concerning the use. E-passport. First, passport demand has nearly doubled between fy-2003 and the current year. In fy-2003 we adjudicated fewer than 7 million passports here in the US. This year, fueled by such as factors as:

- Increasing international travel;
- More naturalizations;

- Americans using their passport as an identity document for reasons other than international travel;
- A growing percentage of Americans renewing their passport at the end of their validity period; and,
- The western hemisphere travel initiative (WHTI—of which I will have more to say later),

The department of state will adjudicate about 13 million passport applications. We expect that number to reach at least 16 million in fy-2007 and perhaps a sustained demand of 17 million or more in fy-2008 and beyond.

I would also like to note that even though "only" 68 million Americans have passports, we are the world's largest issuer of passports and, in fact, process more passport applications than numbers 2 (the U.K.) and 3 (Germany) combined! We're out front and pulling away!!

Another issue that I must emphasize is that a traditional passport is a "globally interoperable" document. Thus, a us. Passport must be able to be read by immigration officials in other countries and we must be able to do the same. There is a U.N... Specialized agency -- the international civil aviation organization or "ICAO"—which helps to ensure international compatibility in travel documents as parts of its dual mission: making air travel secure while facilitating the immigration processing of travelers. Any international effort to improve travel documents is always a "give and take" among nations. We may never come out with what some would view as the perfect solution, but we continue to make progress in ensuring that the person carrying a passport is the person to whom it was originally issued.

Finally, as a little bit of history, I became the department of state's deputy assistant secretary for passport services in January 2003. At that time, I thought that implementing the U.S... E-passport would be a straightforward process. We were well on our way to securing international approval of e-passport specifications and by spring 2003 actually had those largely in hand. I thought that the US. could be in pilot e-passport production within a year to eighteen months and that we would complete the US. transition to a totally electronic passport by the middle of 2005.

I was wrong and I'm here today to talk about that.

What do I mean when I talk about an e-passport and what it will do and cannot do? Each e-passport contains an integrated circuit with a storage capacity of at least 64 kb that operates as a contactless document and consistent with ISO standards 14443a or b. To that chip, the department of state writes the full facial image of the passport bearer, the biometric chosen by the international community. The only biographic information written to the IC is that shown on

the data page of the US passport. We secure the data written through PKI (public key infrastructure).

But that is not all. Additionally, the department:

- Protects the data by including anti-skimming material in the front cover that wraps around onto a portion of the rear cover. This greatly complicates reading the IC as long as the book is closed.
- Adopted basic access control to minimize the risk of eavesdropping. BAC, for those of you not familiar with the term, requires that the data page be read electronically to generate a key that unlocks the IC and allows for an encrypted communication session between the IC and the chip reader.
- Mitigates the risk that an e-passport could be used to "track" the bearer by using a randomized unique id feature in passports issued beginning this summer.

There are a number of things as well that we are **not** doing with the US passport:

- We are **not** collecting fingerscans from American citizens as part of the passport application process, let alone writing those prints to the chip.
- **Nowhere** on the chip or in the passport do we include your social security number, home address, blood type, DNA, telephone or cell phone number or other identity-rich material.

In terms of the design of the US e-passport, I would argue that one of the most important issues for the department of state has been dealing with the reality of biometrics. Biometrics in my opinion is a tool – not a total solution to problems. Vendors and government experts have frequently, I'm sorry to say, oversold biometrics. They help all of us identify suspect travelers or visa and passport applicants. But they are not a panacea in and of themselves.

Thus, in the case of the US passport, we integrate biometrics as a key element of an overall passport security improvement project. But we also:

- Redesigned totally the US Passport. Quite honestly, our existing passport design was dated. As part of the e-passport rollout, we are introducing a new generation passport redesigned literally from cover to cover in terms of both artwork and security features.

- Strengthened the adjudication process. I know that in the case of the US, we need to do a better job at "looking behind the paper" in a passport application. We are making progress by having better access to information in other us. government databases, but we still have more work to do.

As I noted, we include in the US Passport an IC and that obviously raises the issue of radio frequency identification (RFID). In this regard, it is critical to note that the RFID technology in the US Passport operates in a "proximity read" mode only.

When I started working on this project and really up until last spring, I was confident that the IC Could only be read at a distance of 10 cm or less from the reader. The department of state published a notice of proposed rulemaking last spring announcing our e-passport plans. At the same time we were working with our colleagues at the national institute of standards and technology (NIST) to validate this belief. Well, I have to admit that I was wrong. As was demonstrated in NIST testing and by others, it is possible—at a minimum—to activate the IC at a range in excess of 10 cm. This then raises the risk of either data theft via skimming or eavesdropping.

Thus, we went back to the drawing board and adopted a "belt and suspenders" approach to protect the personal data on American citizens that we write to the IC we are doing so by incorporating anti-skimming technology, basic access control and randomized unique id features into our e-passports.

I should also note that some of the claims made about the susceptibility of e-passports to skimming or eavesdropping were overstated. Even in a laboratory setting with highly sensitive equipment we have never been able to activate the chip from a distance of more than a few feet. Moreover, the power requirements go up so quickly—I believe that field strength attenuates according to the cube of the distance—that long range collection is impractical. And, I must emphasize again that the risk mitigation strategy of anti-skimming technology plus basic access control overcomes this risk.

I want to take the opportunity today to thank the US and international privacy community for alerting us to the potential risk of data skimming and eavesdropping. I am confident that as a result of their concerns, we are now issuing a significantly more secure us. e-passport than our original design provided for. And, I believe the US E-passport is at the forefront of international efforts to produce e-passports that minimize the risk of unauthorized reading and identity theft.

Let me end this portion of my remarks by providing a status report on the US E-passport program. And, here I think I have good news. The department of state recently began pilot production of "diplomatic" e-passports. In other words, we are "walking the walk" by serving as our own test-bed for this program. Next month, we will start making "official" e-passports for other government travelers and issue "tourist" e-passports this summer.

I would be happy to answer any questions you may have about the e-passport before I begin my discussion of the western hemisphere travel initiative.

On to the western hemisphere travel initiative or WHTI as I like to call it.

By WHTI I am referring to section 7209 of the intelligence reform and terrorism prevention act of 2004. That legislation mandates that as of 1 January 2008 American citizens reentering the United States after travel in the western hemisphere must present formal documentation to establish their identity and nationality.

As in the case of the e-passport, let me start by providing a few statistics and observations that, I believe, demonstrate the challenge of implementing this program.

According to research which state commissioned, about 6 million Americans who do not have a passport will need to be formally documented to travel to the Caribbean, Canada or Mexico by air or sea; there is also a recurring new demand of about 1 million such travelers per year. For cross-land border travel to Mexico or Canada, we have determined that 27 million Americans will need to be documented formally during the next five years.

In terms of observations, one critical point is that American and Canadian citizens traveling in the western hemisphere can now present themselves for entry processing at either country's port of entry carrying a vast range of documentation. In the case of American citizens returning home they can even make a simple oral declaration that they are citizens. Just one number, I think, summarizes the current situation—Americans often present domestically issued birth certificates to prove their citizenship. However, there are some 8,000 different types of birth certificates currently used by American citizens. I believe it is impossibility for any border inspector to understand the security features of all of those documents and to make, in a few seconds, a decision about the validity of a birth certificate that he or she may have never before seen.

The WHTI program involves a partnership between the departments of state and DHS. The two departments see WHTI as an opportunity to strengthen us. Border security while facilitating the movement of legitimate travelers across our borders.

We at state have great experience in adjudicating applications for travel documents. DHS, of course, is responsible for the processing of travelers at ports of entry. Expressed most basically, what state makes, DHS has to be able to read. Thus, rulemaking for this program is joint. We published last summer an advanced notice of proposed rulemaking (ANPRM) to notify the public formally about our plans to implement this program and to solicit suggestions about how we could improve that process. Also, the two departments have an

extensive public outreach program to educate all concerned about the significant changes coming to us. Travel over the next two years.

In terms of deadlines for the WHTI, there is one overarching requirement—that the program be implemented as of 1 January 2008. To make that happen, state and DHS have proposed to introduce this program in two phases:

- As of 1 January 2007 for travelers returning by air or sea from Canada, Mexico or the Caribbean;
- As of 1 January 2008 for travelers returning across us. land borders with Canada or Mexico.

By the way, please note that neither phase has yet been implemented. If you are planning a getaway to the Bahamas or Bermuda, you do not need a passport to meet the requirements of the WHTI. However, in today's world, many airlines and cruise lines have implemented requirements of their own, so please check with your carrier before you leave for the airport or the dock!!

As I noted earlier, we have issued an ANPRM and have spoken before dozens of groups representing the interests of those affected by WHTI. Coming out of those discussions and the public comments on the ANPRM is a shared recognition by state and DHS that the traditional book style passport appears to be the appropriate document for travel by air and sea regardless of destination. However, to address the frequent travel by those living and working on the land borders, we need to develop an alternative to the traditional passport. We have spent the last several months designing a "passport" card that will have the following features:

(1) Adjudicated by the department of state to the exact same standards applied to a traditional book-style passport;
(2) Serve as proof of identity and nationality;
(3) Pocket sized;
(4) Considerably less expensive than a traditional book-style passport; and,
(5) Designed to make our borders more secure while at the same time facilitating the processing of travelers through us. Ports of entry.

In partnership with DHS, we have resolved most of the issues concerning the development of the card. However, there is one major issue standing between now and the release of a request for proposal (RFP) for assistance in implementing this program -- which technology should be incorporated into the card to facilitate border processing of travelers while protecting data privacy?

Vicinity-read technology is currently used by DHS in some of its voluntary programs for border crossers and clearly has significant potential in terms of travel facilitation. At the same time, some experts, even from the RFID manufacturing community, have expressed concerns that vicinity read

technology may present privacy vulnerabilities or at least the appearance of such vulnerabilities. Other technologies such as proximity-read RFID may offer security advantages, but may not have all of the travel facilitation benefits that we are needed to make our borders both more secure and smarter. And, there are other ideas—such as vicinity-read technology that would be provided in an anti-skimming pouch or even cards that could be turned on or off at the push of a button--that we are looking at.

I cannot say with any certainty which technology we will choose. But I can say two things without doubt. One is that the department of state will go thru a rule-making process that will explain our technology choice. Any and all concerned are encouraged to comment during that rule-making process regarding the technical solution that we propose. Second, we have to make soon a decision on this technology issue so that state can issue early this spring an RFP for the assistance we need to implement this program.

In closing, if anyone would like to see a US. e-passport or a prototype of our travel card, I have both with me. Please see me after this session.

Thank you for your attention. I look forward to your questions.