

**Before the
US STATE DEPARTMENT
Washington, D.C. 20037**

Regarding)	
)	RIN 1400-AC22
The US Department of State's)	Public Notice 5558
Request for comments on the Notice of)	Docket ID: DOS-2006-0329
Proposed Rule Making (NPRM), Public)	
Notice 5558, regarding technology)	
Standards used for the card-format passport)	
Required by the Western Hemisphere)	
Travel Initiative)	

**COMMENTS OF THE SECURE ID COALITION
TO THE DEPARTMENT OF STATE
REGARDING
THE NOTICE OF PROPOSED RULE MAKING,
"CARD FORMAT PASSPORT."**

The Secure ID Coalition is pleased to submit the following comments as part of the State Department's **Notice of Proposed Rulemaking (NPRM) [Public Notice 5558]**. Public Notice 5558 asked for input on the proposed land border passport card required as part of the Western Hemisphere Travel Initiative. The passport card is expected to work within the People Access Security Service (PASS) system.

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents, including contactless smart cards. Our mission is to promote the understanding and appropriate use of smart card technology that achieves enhanced security for ID management systems while maintaining user privacy. Consequently, our coalition welcomes this public comment process to express our concern with the NPRM selection of card architecture that as proposed will open vulnerabilities in both the privacy of U.S. citizens and the security of the U.S. borders.

It is the Secure ID Coalition's strong recommendation that the Department of State (State) and Department of Homeland Security (DHS) rethink the use of an embedded Radio Frequency Identification (RFID) tag conforming to the International Standard Organization (ISO) 18000-6C standard commonly known as EPCglobal Generation 2 – UHF RFID, as it will not meet the necessary policy requirements for any personal identity management system.

The Secure ID Coalition commends the State Department on the successful roll-out of the new e-Passport and the policy process that occurred to ensure the protection of our

national security and citizen privacy. That process relied on consultation with stakeholders on industry standards and best practices, included extensive testing of technologies and products, and incorporated adjustments to design specifications as a result of public concerns regarding privacy. We believe that to replicate that successful roll-out, State and DHS should acknowledge the concerns about privacy that have been raised by ID management industry experts and by the U.S. Congress.

Our National Security

Originally passed to protect our borders and provide security for our nation, the Western Hemisphere Travel Initiative (WHTI) established the foundation for border crossing documents to ensure those coming into the U.S. were presenting authentic documents and that Customs and Border Protection (CBP) could verify those individuals were who they claimed to be. This policy seeks to secure our nation's borders by providing as much information as possible about those travelers entering the U.S. Unfortunately, the implementation as defined in this NPRM will neglect the primary objective of the WHTI program – security.

EPCglobal's Generation 2 – UHF RFID is a technology that was developed for and is used in supply-chain management applications to track products and pallets within a defined area such as a distribution warehouse. The sole purpose of the Gen 2 RFID chip is to be found and read. As a result, the tag's simple numerical identification number is broadcast openly for ease of organization and tracking. If the vendor wanted to incorporate a security feature the best they could offer would be a simple "password" that would be insecurely conveyed in the RF protocol. In such a supply-chain management application, Gen 2 RFID is an excellent technology. However, in an identification document intended to be carried by U.S. citizens, radio frequency technologies must incorporate security features that are strongly resistant to ID fraud, tampering, counterfeiting and terrorist exploitation. To date there is no evidence that Gen 2 RFID can adequately incorporate these features into their identification card product.

As the passport card would be implemented in real life and as proposed in the NPRM, travelers desiring to enter the U.S. through the land borders will be required to place their individual passport card on the dashboard of their vehicle so that it can be read from a gantry up to thirty feet away. While that might be practical and expedient in a product supply-chain management application, thirty feet allows anyone who possesses an unauthorized reader to read the information on the passport card. Additionally, the ability to clone a card and create a virtual replica is possible and probable. In this instance it would be all too easy to move across a land border with a fraudulent card.

As proposed, the International Standards Organization (ISO) 18000-6C RFID chip protocol lacks the means to electronically authenticate the chip in the document. The purpose of the Intelligence Reform and Terrorism Prevention Act of 2004 is to improve the security of the documents identifying U.S. citizens. The RFID chips proposed for use in the NPRM are vulnerable to skimming, cloning, spoofing, and denial of service attacks that will enable terrorists to exploit these vulnerabilities and render our borders less

secure than could be achieved using appropriate contactless smart card technology based on proven ISO 14443.

The Secure ID Coalition strongly recommends State and DHS focus on ISO 14443 as the card foundation for the passport card. ISO 14443 is the recognized international standard for identity card management and is the only interface that can incorporate strong encryption, mutual authentication and biometrics. Unlike Gen 2 RFID, the security features of ISO 14443 based cards protect the card itself and enable communication between the card and reader to be secured against all the attacks to which ISO 18000-6C tags are vulnerable.

Citizen Privacy

Information associated with an individual is part of the foundation of a citizen's identity. Under the proposed NPRM the passport card would contain a unique identifier – a “static number” – that would point to the database record of the traveler. As implemented, the database look-up number becomes part of the traveler's identity and must be protected with the appropriate security features.

The 18000-6C RFID specification does not provide for strong security features incorporated into these RFID chips because the main priority is convenience in tracking products in a warehouse-type environment. Information on or in the product contained on the RFID tag is not deemed serious enough to protect with strong cryptographic mechanisms. This lack of strong security features, however, opens the proposed passport card to skimming, tracking, duplication, association to an individual and eavesdropping of transactions.

Features that allow for security and privacy protection must be designed into any identification document so that information cannot be transmitted in plain text, resulting in the identity of the citizen or information associated with an identity being intercepted and exploited. Security protections that should be incorporated in the proposed passport card, regardless of the information contained on the card, include: data privacy (encryption), data integrity (digital signature), and card and reader authentication with the optional addition of using biometrics to further ensure the correct person is using the card.

In addition to the RFID chip being read quickly and easily within a large warehouse, it is also usually designed to be read from up to thirty feet away. With any human identification program a thirty-foot read range is a privacy threat to the citizen carrying the card, since information can be read by anyone in the vicinity of the card, with a commonly available (unauthorized) reader that can be purchased over the Internet. The use of ISO 18000-6C RFID chip technology threatens to treat U.S. citizens like products without regard for the privacy protection of their identity.

By issuing this NRPM, the State Department and DHS seem to be ignoring the expertise and work that has been done by the National Institute of Standards (NIST) and

International Civil Aviation Organization (ICAO) on other identity card programs within the federal government and around the world. Many other programs are being implemented using the necessary security and privacy enhancing features for identity credentials. The State Department and DHS are clearly ignoring the established and implemented standards previously developed by NIST and ICAO that will secure the information on identification documents using an RF interface and only allowing for a 4 inch (10 cm) read-range instead of up to 30 feet (10 m).

At the international level expertise from around the globe collaborated to ensure the security of the e-Passport credential resulted in a gold standard for protecting the privacy of citizens. The use of ISO 14443 based technology, as specified by ICAO, has allowed the adoption of several security features that mitigate against unauthorized access to the e-passport credential information. It is a serious privacy and security misstep that State and DHS are now attempting to reinvent the wheel by proposing an incompatible, insecure technology in comparison to that of the e-passports for the proposed RFID based passport card.

Operational parameters of the land border crossing checkpoints are not compromised in any way by the use of ISO 14443 standards based technology instead of ISO 18000-6C technology. In fact, they will improve the credential's security, usability and readability as they will not require removal from physical faraday shields. Transaction times with readers are of no significant difference between the two technologies.

Using ISO 14443 type cards ensures security features are deployed to protect the privacy of the credential, even if only a static ID number is used to access the full credential held in a central database. No faraday shielding is required by ISO 14443 based cards as security features protect against unauthorized access to the information in the card, unlike ISO 18000-6C RFID tags.

Additionally, DHS's own Data Privacy and Integrity Advisory Committee over the past few months has been working on a report addressing the use of RFID in human identification documents. The initial draft was very critical of such careless RFID enabled identification credentials implementations.

The Secure ID Coalition recommends protecting the privacy of U.S. citizens who will be carrying the passport card and ensure that these security features meet the highest level of privacy protection. In addition, we recommend that State and DHS consider carefully the concerns and comments from the Data Privacy and Integrity Advisory Committee and incorporate the Committee's recommendations into any identity credential issued to U.S. citizens.

Infrastructure Investment

Cost is one of the primary considerations in any new program or identity credential implementation. The Secure ID Coalition is concerned that if State and DHS move forward as planned with the proposed passport card, enormous and unnecessary

additional costs will be incurred by forcing border management agencies to invest in different and additional reader infrastructure and back-end systems along the land borders.

Under the WHTI, travelers will either need an e-Passport book or a passport card to enter the U.S. through a land border. The e-Passport books both in the U.S. and around the world comply with the International Civil Aviation Organization (ICAO) standard for travel documents based on ISO 14443, thus creating a common standard to allow for interoperability. Reader infrastructure for the e-Passport will be necessary at the land borders in order to authenticate those travelers carrying e-Passports from the U.S. and other countries.

If State and DHS implement a passport card that is based on different technology than the e-Passport book, multiple different types of reader infrastructure and back-end database systems will have to be deployed, adding significant cost to the implementation.

It is not clear that current reader infrastructure deployed for limited pilot programs using RFID can be adapted from the first generation of RFID to accommodate the reader requirements for Gen2 ISO 18000-6C technology. If the reader infrastructure cannot be successfully adapted, then further additional cost will be required to dismantle current readers and redeploy upgraded infrastructure to operate with the current ISO 18000 -6C RFID requirements.

Competition among Vendors

Under the current proposed NPRM, the Secure ID Coalition is concerned that competition among vendors will be limited, lack openness and not promote non-proprietary systems and component parts.

ISO 14443 is an open international standard that allows anyone to build systems and solutions, ensuring that the widest range of solution providers will participate in a competitive process. ISO 14443 is a mature technology platform with over 20 years experience in the personal identity management sector and widely recognized as the only choice for protecting personal privacy. The solution outlined in the NPRM looks to a technology that was never designed for personal identity management applications. If State and DHS are contemplating the addition of proprietary and unproven features to ISO 18000-6C in order to address some of the many security and privacy issues associated with vicinity technology, then the resulting architecture will most likely be a proprietary solution. Such a solution will lock the agencies into a single vendor, effectively preventing meaningful competition in the procurement process.

Congressional Direction

In the fiscal year 2007 Department of Homeland Security Appropriations bill, signed by the President on October 4, 2006, State and DHS are required to receive certification from National Institute of Standards and Technology (NIST) that the passport card

architecture meets or exceeds ISO security standards and meets or exceeds best available practices for protection of personal identification documents.¹ Counter to the Congressional directive **the NPRM does not reflect any consultation with or certification by NIST.** The congressional language makes it clear that industry best practices for identity management must be considered as part of the passport card program. Equally important, security standards must also be considered to protect the cardholder's privacy. The Secure ID Coalition is concerned that the NPRM does not consider these important Congressional concerns.

The Secure ID Coalition is pleased to provide these comments to the Department of State, and by extension, the Department of Homeland Security. The Western Hemisphere Travel Initiative is critical to our national security and it is our sincere hope that both agencies will seriously consider the security, privacy, cost and competition policy issues confronting the implementation of the passport card program.

Respectfully submitted,

On behalf of the
Secure ID Coalition
919 18th Street, NW
Suite 925
Washington, DC 20006

Kelli A. Emerick
Kelli A. Emerick
President, IT Policy Solutions

December 7, 2006

¹ See P.L. 109-295 Title V, Section 546

About the Secure ID Coalition

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents, including contactless smart cards. Our mission is to promote the understanding and appropriate use of smart card technology that achieves enhanced security for ID management systems while maintaining user privacy.

Coalition members support specific citizen privacy rights as follows:

- ***Privacy*** of personal information as defined by all relevant regulations and laws, principally the body of laws known as *Fair Information Practices*.
- ***Confidence*** that ID documents have been appropriately secured against threats of fraudulent access to personal information.
- ***Knowledge*** of what data is contained in electronic ID documents; how that data will be collected, secured and transmitted; the presence of radio frequency (RF) technology in ID documents; and when, where and why RF devices are being read.

For more information, please visit our website at www.secureidcoalition.org