Privacy Impact Assessment
for the

Use of Radio Frequency Identification (RFID) Technology for Border Crossings

January 22, 2008

Contact Point

Colleen Manaher
Western Hemisphere Travel Initiative Program Management Office
Office of Field Operations
(202) 344-3003

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

U.S. Customs and Border Protection (CBP) employs Radio Frequency Identification (RFID) Technology that is to be used in cross border travel documents to facilitate the land border primary inspection process. A unique number is embedded in an RFID tag which, in turn, is embedded in each cross border travel document. At the border, the unique number is read wirelessly by CBP and then forwarded through a secured data circuit to back-end computer systems. The back-end systems use the unique number to retrieve personally identifiable information about the traveler. This information is sent to the CBP Officer to assist in the authentication of the identity of the traveler and to facilitate the land border primary inspection process. Multiple border crossing programs use or plan to take advantage of CBP's vicinity RFID-reader enabled border crossing functionality including CBP's own trusted traveler programs, the pending Department of State's (DoS) Passport Card, the Mexican Border Crossing Card, the proposed Enhanced Driver's License (EDL) offered by various states, tribal enrollment cards that could be developed by various Native American Tribes, and the proposed Enhanced Driver's Licenses being developed within the various provincial authorities in Canada.

Introduction

This PIA addresses the use of vicinity RFID in CBP's border crossing program. Separate PIAs and various System of Records Notices (SORNs) address the details of the specific border crossing programs that use vicinity RFID technology as part of the cross border travel documents associated with those programs. CBP's trusted traveler programs[1] (TTP) are currently in operation and are covered by the PIA for the Global Enrollment System (GES) which is available on the DHS Privacy Office's website: www.dhs.gov/privacy. The programs for the DoS Passport Card, Mexican Border Crossing Card, State EDL programs, the Canadian provincial driver's license programs, and the possible tribal enrollment card provided by various Native American Tribes are still being developed. A PIA for these programs will be published prior to the programs' use of RFID technology to facilitate border crossing.

To receive an RFID-enabled border crossing travel document (RFID card)[2] individuals must submit an application to the particular border crossing program and, for CBP's Trusted Traveler's Program, pass a CBP background check.[3] State EDLs, DoS's Passport Card, and the

[1] This term is also used in the GES PIA. The term "trusted traveler" program(s)" also includes all programs designated by DHS and/or CBP as "registered traveler" programs. "Trusted traveler" and "registered traveler" programs typically require the same or similar types of personal information to be submitted, in advance, by an individual The difference between the two types of programs is that "trusted traveler" programs require a greater level of vetting and screening of its participants.

[2] This PIA does not pertain to the Department of State's issuance of the traditional passport book.

[3] For example, in CBP trusted traveler programs, applicants, generally, will not qualify for participation in a trusted traveler program if they: provide false or incomplete information on the application; have been convicted of any criminal offense or have pending criminal charges to include outstanding warrants; have been found in violation of

Mexican Border Crossing Card do not require background checks to be conducted by CBP at the time of application. Once approved through a border crossing program, individuals will receive an RFID card associated with that program that contains a unique RFID number. This number will not contain personally identifiable information (PII), will not appear on the face of the card, and will only be associated with the individual traveler within secured back-end computer systems. In all RFID enabled border crossing programs, the RFID number will only be used to identify the relevant records in secured back-end systems. Once the associated record is identified, information from that record will be used to initiate the border crossing screening process and create a new record of the traveler's border crossing using the database within the Treasury Enforcement Communications System (TECS) that is being transitioned into the Border Crossing Information System (BCIS).[4] In addition, the Automated Targeting System (ATS) will be used for data pertaining to the screening result from clearing the traveler, as an interface for the results of License Plate Reader screening at the land border. Results of these queries will be presented to the CBP Officer to use during the in person border crossing screening process.

RFID systems operate using three components: the RFID tag, the reader, and the back end system. The tag is attached to the object of interest, here the cross-border travel document and contains a number that is unique to that tag. As the tag crosses a threshold (here, the border) the reader triggers the transfer of the unique number from the tag and, through the back end system, associates that number with other information that creates a meaningful response to the observation of the tag crossing the threshold. There are two types of passive RFID technology: Proximity RFID for closer range transmissions (3-6 inches) and Vicinity for longer range transmissions (between 20-30 feet). Documents issued by DHS (and by DoS in response to WHTI) use vicinity RFID technology to permit a more efficient pre-positioning of the traveler records. While the individual traveler is in line to cross the border, the RFID reader triggers the wireless transmission of the RFID tag number from the RFID card, provides the ID number to backend computer systems that identify the appropriate record(s) and makes them available to the CBP Officer before the traveler reaches primary inspection. The number also triggers automated checks against appropriate law enforcement databases and watchlists. When the individual traveler reaches primary inspection, the relevant border crossing information is already pre-positioned on the CBP Officer's computer screen and the Officer can be properly prepared to either process the border crossing more quickly or be ready to refer the traveler to secondary to address any derogatory information related to the individual traveler.

---

any customs, immigration, or agriculture regulations or laws in any country; are subjects of an ongoing investigation by any federal, state, or local law enforcement agency; are inadmissible to the United States under immigration regulation, including applicants with approved waivers of inadmissibility or parole documentation; or cannot satisfy CBP of their low risk status or meet other program requirements.

[4] The System of Records Notice for TECS is published at 66 FR 53029.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The only information collected via a CBP RFID reader at the border is the RFID identification number of the RFID chip embedded in the document used to cross the border. The RFID number consists of a unique number issued by the issuing authority of the RFID enabled card. The unique number in the RFID chip does not contain any information that is personally identifiable to that traveler. The RFID number of the card is associated with the unique enrollment record created for the individual traveler as part of a program to permit border crossing.

Additional information is collected during the DHS enrollment process for each DHS border crossing document. This information is collected during the application process and is associated with the RFID enabled card number. When the RFID enabled card is read during the border crossing, the RFID identifier is used as a reference to the enrollment information as well as other information associated with the border crossing clearance process. The only information transmitted via RFID when crossing the border is the RFID number.

There are two generations of RFID tags, each has a particular configuration of RFID numbers. The first generation RFID tag, Gen 1, uses a single string of numbers. The second generation RFID tag, Gen 2, separates the tag number into several parts. One part identifies the tag as a travel document, another part identifies the type of tag (*e.g.*, the issuing State for EDL or issuing agency for a federal travel document), and another part is a unique number assigned to the file containing biographic and biometric information about the person. Lastly, the tag possesses a unique number assigned solely to the RFID chip for control purposes. Currently, CBP's trusted traveler programs use Gen 1 tags[5]. Gen 2 tags are used for many other purposes (to identify many other types of objects) and are based on standards developed by EPCglobal. In the future, the CBP trusted traveler programs will use Gen 2 tags as will the other documents that could be used for crossing U.S. borders (DoS's Passport Card, State EDLs, and Tribal cards). This means that when the Gen 2 tag data is sent from the RFID card to the RFID reader, CBP will be able to identify the type of card in terms of providing a numeric identifier that can be associated by the back-end computer system with the particular issuer of the border crossing card (e.g., DoS, TTP, state (EDL), tribal, and Canadian cards).

Additional personally identifiable information is printed on the face of the trusted traveler card and is used by the CBP Officer as part of the clearance process for the border crossing of each traveler. For example, the CBP trusted traveler cards include the following information: *on the front of the card*: Surname, Given Name, Middle Name, Gender, Citizenship, Date of Birth, Expiration Date, Photo and Travel Document Number; and *on the back face of card*: ID, and, as

[5] It is expected that CBP's Trusted Traveler Programs will be issued with Gen 2 tags in the near future.

of November 2006, MRZ information that includes the written information from both the front and the back of the card.

1.2 From whom is information collected?

Information is collected from all travelers, both U.S. persons and foreign nationals, who obtain an RFID-enabled border crossing document. While travelers may cross the border without a vicinity RFID enabled travel document, they must still provide biographical data, either from their passport or other approved travel document. During enrollment in a program that issues an RFID enabled travel document, sufficient personally identifiable information is collected from the individual to determine eligibility to use this card for border crossing purposes. The border crossing travel document assigned to the traveler following enrollment contains an RFID chip with a unique ID number preceded by a header that identifies the issuing authority of the card. During border crossings, CBP collects the RFID number and header from the RFID enabled cross border travel document assigned to the individual during the aforementioned enrollment process. For non-DHS issued documents that are RFID enabled, DHS will receive information associated with the RFID number which will reference biographical and biometric (photo) information maintained in the issuing entities back-end database. Issuing entities could include state Department of Motor Vehicles (DMV) for enhanced driver's licenses or tribal authorities for Tribal cards.

1.3 Why is the information being collected?

CBP collects the RFID numbers so that it may access data pertaining to the traveler from back-end systems to verify the identity and citizenship of travelers as they cross the border. CBP and its legacy predecessors at the border, the U.S. Immigration and Naturalization Service and the U.S. Customs Service, have always possessed the authority and discretion to inspect and identify persons crossing the border for reasons of national security and law enforcement. As a result of the Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA) and its implementation, this mission is being expanded to mandate that CBP identify and collect information pertaining to citizenship with respect to all persons crossing the border. The unique RFID number embedded in the cross border travel document is collected via wireless transmission from the card to the RFID reader as part of the clearance process at each border crossing. The RFID number is used to retrieve the personally identifiable information from the back-end systems and present that information for the CBP Officer. The RFID identifier is collected while the traveler is in line for the inspection booth so that the additional information can be pre-positioned for the Officer's review before the traveler reaches the Officer. Pre-positioning the information facilitates faster border crossings, permits visual verification of identity using the photo presented from back-end systems, and enables the Officer to prepare for the traveler should any derogatory information be retrieved from the back-end systems.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

This PIA addresses the use of RFID enabled cards as part of CBP's processing of a border crossing event. Participation in CBP RFID enabled border crossing programs, is governed by the Immigration and Nationality Act, specifically sections codified at 8 U.S.C. §§ 1101, 1103, 1182, 1185, 1201, 1304, and 1356, and implemented by title 8 CFR section 235.7.[6] Use of DoS's passport card, individual State EDLs, or other approved RFID card is an alternative means of satisfying the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004, which removes the exemption for U.S. Citizens and certain foreign nationals within the Western Hemisphere from presenting a passport at the border upon entry into the United States.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The privacy impact analysis in this section of the PIA focuses on the nature of the RFID information. The privacy analysis in the next section focuses on the use of that information (the wireless transmission of the information via RFID).

To minimize potential privacy impacts, RFID enabled cards used in CBP's processing of a border crossing event contain only a limited amount of information that is presented by the RFID transmission process. The only information exchanged in the RFID portion of the border crossing event is the unique number assigned to the RFID enabled card by the card manufacturer. While this unique identifier will eventually be associated with a particular traveler, at the time the RFID number is created it is not generated or based in any way on personally identifiable information related to an individual traveler, although the number does contain information pertaining to the issuing authority. All personally identifiable information used in the border crossing clearance process is stored in secured systems and on a secured computer network. Since only the RFID number is transmitted, the risk of revealing personally identifiable information about the traveler via RFID is severely limited.

There are privacy risks that are associated with the nature of the RFID number: Cloning, Secondary Uses, Tracking, and Profiling. The following is a description of each of these privacy risks along with CBP's mitigation of those privacy risks. Section 2.4, below, discusses the potential privacy impacts presented by the way the RFID number is used, specifically, those privacy risk associated with the wireless transmission of the RFID number.

[6] Individuals eligible for CBP's trusted traveler programs include U.S. citizens, lawful permanent residents of the United States, and citizens of Mexico, Canada, and other nations who travel frequently to the United States. Non-U.S. citizens must have valid entry documents, be admissible to the United States, and demonstrate they are low risk travelers by providing certain documents called for by statute and regulation

Cloning. Cloning is the illegitimate duplication of the information stored in the RFID tag portion of the RFID enabled card. Cloning raises three potential privacy risks: first, that personally identifiable information could be copied from the RFID enabled card, second, that someone else could use the cloned RFID tag to claim the identity of the legitimate traveler, and third that the use of multiple cloned RFID enabled cards could overwhelm the CBP RFID reader. RFID enabled cards for border crossing mitigate these privacy risks by storing no personally identifiable information in the RFID tag and by only using the RFID number that is transmitted wirelessly to retrieve from back-end systems the personally identifiable information used during the border crossing event. CBP Officers only compare the data from the back-end systems, the information on the face of the card, and the physical inspection of the individual traveler as the basis of the clearance process. If the RFID number is cloned and used during CBP's border crossing process, the back end system will use the RFID number, which contains a permanent "Tag Identifier," serial number programmed at the time of manufacture, to retrieve the legitimate traveler's records (photo and biographic data) which will not match the traveler using the cloned RFID number and the CBP Officer will detect illegitimate use. Lastly, CBP's mitigation, in the event that multiple cloned cards are employed to overwhelm the capacity of its reader, is to turn off the overloaded system and process travelers using those non-RFID aspects of the RFID enabled card (*i.e.*, printed biographical data and photo) that support manual clearance at the border.

Secondary Uses. Secondary Use is the repurposing of the RFID number for some other program or by another agency or commercial organization. Secondary Use raises the potential privacy risk that the RFID number would be used for alternate purposes without the informed consent of the individual. CBP mitigates these privacy risks through a published SORN (*e.g.*, for CBP Trusted Traveler Programs the published SORN is the Global Enrollment System (GES) SORN, published at 71 FR 20708) that notifies the public of the permitted uses of the border crossing enrollment data and transaction information and limits the lawful use of the information, maintained in the SORN, to those stated uses and others that are compatible with the purpose for the original collecting of the information. Any use not specified in the SORN, or compatible with its stated purpose, is a violation of the Privacy Act and contrary to CBP policy. To utilize RFID enabled cards as part of CBP's border crossing process, all entities will be required to establish legally enforceable restrictions on the use of the RFID number that meet the same standards and parameters set by CBP.

In addition to the legal restrictions, CBP educates individuals enrolling in CBP's RFID enabled border crossing programs regarding the permissible uses of the RFID card (and thus the number) and supplies individuals with a protective sleeve that blocks the transmission of the RFID number from the RFID enabled card. This provides the individual with the ability to control when the RFID number would be read. These same protections will be recommended

and, where possible, required for all participants using RFID enabled cross border travel documents.

Tracking. Tracking is a form of secondary use that exploits the uniqueness of the RFID number to associate a specific individual with specific places over time. Tracking raises the potential privacy risk that an individual carrying an RFID enabled cross border travel document would unknowingly become the subject of surveillance and profiling or be simply providing information about his or her possession of an RFID enabled card and from whom it was issued. CBP mitigates this privacy risk by educating individuals obtaining an RFID-enabled travel document regarding the permissible uses of the RFID card (and thus the number) and supplies individuals with a protective sleeve that blocks the transmission of the RFID number from the RFID enabled card. CBP strongly encourages all other issuers of RFID enabled cards, similarly, to provide protective sleeves for storing the respective RFID enabled card when it is not being used by the individual. This provides the individual with the ability to control when the RFID number would be read. These same protections will be recommended and, where possible, required for all travelers using the vicinity RFID enabled border crossing documents.

Profiling. Profiling is the reconstruction of a person's movements or transactions over a specific period of time to ascertain something about the individual identity. Profiling raises the privacy risk that PII could be collected about the individual without the individual's knowledge. CBP mitigates this risk by not transmitting or receiving PII through RFID. The only information that is transmitted wirelessly is the RFID number, which does not contain PII.

The new RFID tags to be used in the CBP border crossing documents (Gen 2 – see discussion in section 1.1, above) do contain header information which could reveal some overall category information, that is the type of RFID enabled card being carried.

The education and protective sleeve described above mitigates the risk of unintended uses of the RFID number by empowering the individual traveler regarding when the RFID number is transmitted. In addition, the border crossing environment (the only location where the RFID card is intended to be used) is physically controlled by CBP to prevent unintended access to the RFID number.

Another potential risk is that the RFID number could be used to access the back end system and reveal the PII contained in those systems. CBP mitigates this risk by the security procedures applied to the communication connections between the CBP Officer's computer terminal at a field location and the back-end system resident on CBP computers at the CBP National Data Center.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The RFID number in the RFID enabled card is transmitted wirelessly to CBP's RFID readers to facilitate the processing of individuals. The only information transmitted wirelessly is the RFID number described in Section 1, above, and that number is only used to retrieve from the secured back-end systems those records pertaining to the individual. Retrieving those records while the individual is still in line enables the CBP Officer to pre-position PII related to the individual and begin the screening process before the individual arrives at the primary inspection booth.

CBP only uses the RFID number to retrieve the records associated with the individual traveler during the border crossing. At this time, CBP intends no other uses, other than during the border crossing experience, of the RFID enabled card or the RFID number.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

No. The use of the RFID identifier is limited to enabling a CBP Officer to access PII maintained in secured back-end systems for the express purpose of aiding the inspection of the individual crossing the border.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

When the traveler reaches the point in the primary inspection line where the RFID reader is positioned, the RFID reader collects the unique RFID number from the RFID enabled card and then pre-positions PII from the back-end systems corresponding to the individual. During the in-person physical inspection, the CBP Officer compares the information on the screen with the information on the face of the RFID enabled card and the traveler. If information on the CBP's computer screen, including photo(s) of the individual retrieved from the back-end systems matches the traveler, then the information is determined to be accurate. If the PII retrieved does not match the information on the card and the traveler, the accuracy of the information will be questioned and the Officer will re-scan the identification card. If the information still does not match the traveler, the traveler will be referred for further inspection.

CBP developed procedures to address situations in which a traveler has the same or similar name as someone on a watchlist. TECS was updated in February 2006 to allow CBP officers at ports of entry to eliminate inspections on subsequent trips in cases where travelers' names, birthdates or other biographical information matches those of high-risk individuals once

CBP verified that the individual is not the person of interest. No action is needed from the individual. There is no additional data collected on the individual beyond what is normally collected during a secondary type examination. TECS will block those other records from appearing on subsequent encounters with the individual. This upgrade alleviates additional screening procedures for passengers who have been misidentified due to the same or similar biographical information as watch-listed individuals.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The privacy impact analysis in this section of the PIA focuses on the use of the RFID number discussed in Section 1, above. There are privacy risks that are associated with the wireless transmission of the RFID number: Skimming, Eavesdropping, and Denial of Service Attacks. The following is a description of each of these privacy risks along with CBP's mitigation of those privacy risks.

Skimming. Skimming is the use of an unauthorized RFID reader to read the RFID number from the RFID enabled card. Skimming raises the privacy risk that PII related to the individual (such as a license plate number) could be gathered and associated with the RFID number without the individual's knowledge or consent. CBP mitigates this risk by physically securing the border environment sufficient to prevent the presence of an unauthorized reader within range to read the RFID enabled cards. CBP also recommends and, where possible, requires that the only information subject to transmission on an RFID enabled card is the RFID number.

In addition, during the enrollment process, CBP educates all individual RFID enabled card holders to only use the RFID enabled cards during the border crossing event and to use the supplied protective shields to prevent skimming during all other times. CBP will recommend other participants in RFID enabled border crossing programs to supply the same level of education and physical protections.

Eavesdropping. Eavesdropping is the interception of the communication between an RFID reader and an RFID enabled card. Like skimming, CBP's principal mitigation to eavesdropping is its physical control of the border crossing environment. CBP places its RFID readers within a physically protected area that is sufficiently large that an RFID reader placed outside the protect area would not be able to intercept the wireless communication from the RFID enabled card to the RFID reader. During the CBP issuance process, each individual will be encouraged to keep the RFID enabled cards in a secure location and be informed on the proper use of the protective sleeve, the combination of which reduces the opportunities for

eavesdropping by limiting the wireless transmission of the RFID number to the border crossing event within the CBP protected border environment. DHS will recommend that other issuing agencies develop similar recommendations based on the overall use of the travel document, as certain travel documents may be used for purposes beyond border crossing and so recommendations may need to vary.

Denial of service. A denial of service attack could disrupt the RFID communication process either by using a "kill" command which renders a tag permanently inoperable or through an attack that interferes with the transmission of RFID number to the RFID reader. CBP mitigates this risk by physically controlling the border crossing environment to prevent interference with the RFID communications.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

CBP will retain the RFID number that is transmitted during the border crossing for the same length of time that it maintains the biographical and biometric (photo) information to which the RFID number links or points. RFID numbers, generally, are actively used, by CBP, for a period of five years in connection with a cross border travel document. After a period of up to five years, the individual traveler receives a new cross border travel document. The active duration of an RFID number may be less than five years if the traveler chooses not to carry or is no longer eligible for the RFID-enabled document.

This does not mean that the association of the RFID number with the traveler's biographical/biometric information is purged upon removal or withdrawal of the traveler. Individual border crossing records, consisting of information collected at the time of a traveler's crossing of the border, is retained generally, for twenty years, or for investigative purposes, a longer period of time. For example, each individual enrolled in CBP's trusted traveler programs receives an RFID enabled card with a new RFID number every five years as part of the required re-enrollment process. Information maintained in the Global Enrollment System, the database which maintains trusted traveler information, is retained for three years after the ceasing of participation in a trusted traveler program. The retention period for the DoS's passport card is currently under review by the State Department. Similarly, the RFID number in the EDL or other RFID enabled card will be subject to the legal requirements binding upon those issuing authorities, outside the control of DHS. CBP will retain the RFID number, that it collects, for these other participants for the same time period that it retains all information collected during the processing of a traveler crossing the border. The additional information collected during issuance follows a different retention schedule. For example, in CBP's trusted traveler programs (biographical and biometric information) will continue to be maintained in GES and IDENT, subject to updates provided during the re-enrollment process. Pursuant to the System of Records

Notice for GES, 71 FR 20708, records containing biographic information about the individual will be destroyed three years after either the denial of an application as a trusted traveler or a person who participates in a trusted traveler program withdraws from the program. Records containing biometric information will be retained for 75 years in accordance with the terms of the IDENT SORN, 71 FR 13987.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

CBP is working with the U.S. National Archives and Records Administration (NARA) to develop a retention schedule for the RFID number as well the back-end systems. This schedule will be closely aligned with program requirements and will be coordinated with the retention policies and notices of the other participants in CBP's RFID border crossing programs.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Retaining an accurate RFID number for as long as the traveler is enrolled in the trusted traveler program is essential to maintain the integrity of the trusted traveler programs. The additional information collected during the enrollment period follows a different retention schedule based on different criteria. For example, currently, in addition to the information stored in GES and IDENT, information stored in BCIS and TECS is retained for a minimum of twenty and seventy-five (75) years, respectively, to permit the cross-referencing and review by CBP analysts of historical data relating to individuals crossing the border. This additional retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

As a routine practice, the RFID number is not shared with any other DHS organization. CBP intends to maintain the RFID number in a discrete field associated with the biographical information establishing the border crossing record, the RFID number will not be subject to general access. Within one of CBP's back-end systems, GES where the RFID number is stored, access to the RFID number is limited to a limited population of CBP personnel authorized to manage and maintain GES. The border crossing information associated with the RFID number may be shared on a "need to know" basis with such internal organizations as ICE, CIS, TSA, and I&A, but generally the border crossing information and not the RFID number is what is needed.

Data sharing requests for the RFID from internal organizations, such ICE, CIS, and I&A would be reviewed on a case-by-case basis and be vetted to meet specific "need to know" criteria.

It is anticipated that the RFID number for the DoS passport card program will be maintained in TECS. The sharing of TECS information is controlled by CBP in conjunction with DoS and will be shared on a "need to know" basis consistent with the SORN published for TECS, 66 FR 52983, 53029. The RFID number for EDLs and Tribal cards will be retained as a discrete field in the record representing the border crossing event.

4.2 For each organization, what information is shared and for what purpose?

The RFID number associated with a border crossing record will only be shared on a "need to know" basis consistent with the Border Crossing Information System (BCIS) SORN. PII other than the RFID number that is contained in a border crossing record, will be shared throughout DHS consistent with the receiving entities function within the DHS mission, a law enforcement purpose, or on a need to know basis.

4.3 How is the information transmitted or disclosed?

The RFID number may be transferred either electronically to populate back-end systems that will use the RFID number to retrieve additional information related to the traveler, or on printed materials to authorized personnel. Such printed records could include investigative reports or system performance analyses.

The only wireless transmission of the RFID number occurs at the border as part of the border clearance process. CBP's trusted traveler identification cards are not used for any other purpose and travelers are provided education regarding how best to prevent unintended transmissions of the RFID number outside the border crossing environment. The RFID numbers in other RFID enabled travel documents (DoS's passport card, State EDLs, and other RFID capable ID cards) are not used by CBP for any purpose beyond the border crossing function.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

To mitigate the privacy risks of PII being used inappropriately, all DHS personnel requesting information from an RFID enabled card, including the RFID number, must establish a need to know the information as part of official employment responsibilities. Additionally, any internal DHS access to the data is controlled by CBP through the use of strict access controls for the users, passwords, background checks for individuals accessing the data as well as system audits that track and report on access to the data.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Two of CBP's trusted traveler programs, NEXUS and FAST-Northern Border are bi-lateral programs between the U.S. and Canadian Governments. PII collected during enrollment and the associated RFID number from these two programs is shared with the Canadian government to allow for the use of the same RFID card for each country's border crossing programs. Limited information is also shared with the Mexican Government, see section 5.2, below.

CBP has set up a system such that the sharing of the RFID number is more restrictive than the general border crossing information that is collected along with the RFID number. Sharing will occur in conformance with the Privacy Act System of Records Notice, which for the trusted traveler program would be GES and for all other collections would be the Border Crossing Information System.

In the instance of use of the DoS Passport Card and Mexican Border Crossing Card, State EDLs, or other RFID capable ID card, information may be shared with the issuing authority regarding individual border crossing instances where the governmental entity, external to DHS, has established a law enforcement purpose for its request.

5.2 What information is shared and for what purpose?

The NEXUS Programs and FAST- Northern Border are bi-lateral programs between the United States and Canadian Governments. Application information and the RFID number are shared between the two countries, to allow for the use of the same RFID number for each countries trusted traveler database.

The Mexican Government has the technical capability to send RFID number readings on the FAST card and is provided with either a "valid card" (green light) or "not valid card" (red light) response. However, Mexican authorities currently do not have the infrastructure to read the FAST RFID number and CBP does not share any applicant information with Mexico – just status pertaining to the validity of the FAST RFID card. With regard to the Mexican Border Crossing Card, application information and the RFID number are shared between the two countries, as Mexico is the issuer of the card.

The biographical information from BCIS that is referred from back-end systems through reference to the RFID number is shared with agencies outside DHS. This biographical information is shared subject to the same restrictions regarding 'need to know' and law

enforcement purpose as exist for internal sharing within DHS. Similarly, where a specific purpose and need are identified, the RFID number may also be shared on a case-by-case basis.

5.3 How is the information transmitted or disclosed?

Enrollment information from CBP's trusted traveler programs, including the RFID number is shared between the United States and Canada via secured data interface. In the future, as other participants in the RFID border crossing program are added, communications between CBP's system and the systems of those participants will also be conducted via secured data interfaces.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

CBP entered into a *Memorandum of Understanding for the Disclosure of Information for the Purposes of the Joint Alternative Presentation and Inspection Programs* with Canada Border Services Agency that covers the exchange and sharing of information for NEXUS and FAST-Northern Border.

CBP also has a *Customs Mutual Assistance Agreement* with the Government of Mexico and the Government of Canada that includes the sharing of information for law enforcement purposes.

Authorization for outside entity access or interface to TECS and BCIS is granted by the TECS Program Manager and authorized via a MOU between CBP and the outside entity and an Interconnection Security Agreement (ISA) specific to each interface implemented with that entity. The MOU specifies the general terms and conditions that govern the use of the functionality or data, including privacy related limitations on use. The ISA specifies the data elements, format and interface type to include the operational considerations of the interface.

Similar Memoranda/Agreements will be entered into between CBP and other participants of CBP's RFID border crossing program before RFID or enrollment data is shared.

To date, DHS has signed MOAs regarding EDLs with the states of Washington, Vermont New York, and Arizona. Discussions with other states are on-going. The Canadian province of British Columbia (BC) also plans to issue an EDL. To facilitate this and other Canadian provincial enhanced driver's licenses and identification cards, it is anticipated that memoranda of agreement will be signed for the purposes of information sharing between BC and the Canadian Border Services Agency, and between CBSA and CBP.

5.5 How is the shared information secured by the recipient?

Access to data held by CBP, including the RFID number, is controlled through administrative passwords and restrictive rules regarding access to the CBP network and databases. Within each of CBP's back-end systems, users are limited to the pre-defined roles that limit access to data and operations within each system. In the event that information is shared by CBP, such information sharing is governed by the terms of the relevant agreement between CBP and the recipient. The terms of the MOUs/MOAs require that recipient agencies must employ the same or equivalent security protocols and safeguarding means as those utilized by CBP.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

CBP requires all external users of TECS, BCIS, or systems which interface with TECS to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in the TECS database. This includes access to the systems that process the RFID numbers.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Access to CBP data, including the RFID number, is governed by "need to know" criteria requiring the recipient demonstrate the need for the data before access or interface is granted. As noted above, general access to the RFID number will be more limited than access to the border crossing information. The reason for the interface request and the implications on privacy related concerns are two factors that are included in both the initial and ongoing authorization (MOU and ISA) that is negotiated between CBP and the external agency that seeks access to CBP data. The MOU specifies the general terms and conditions that govern the use of the functionality or data, including privacy related limitations on use. The ISA specifies the data elements, format and interface type to include the operational considerations of the interface. MOUs and ISAs are periodically reviewed and outside entity conformance to use, security and privacy considerations is verified before Certificates to Operate are issued or renewed. The same standards for security and privacy that are in place for CBP will be applied to all other participants.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Information on the use of RFID technology is presented to the applicant during enrollment or application. This practice is currently in place as part of the CBP trusted traveler programs and will be implemented for other DHS programs that issue an RFID enabled document. It will be recommended for non-DHS programs as a uniform privacy practice.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. While, the CBP trusted traveler programs are voluntary and use of the other participating cards (DoS passport card, State EDLs, or other RFID enabled ID cards) are not mandated by law, the requirement to provide biographical information upon crossing the United States border is mandatory. Once fully implemented, the Western Hemisphere Travel Initiative (WHTI) will also restrict the manner in which such information may be presented. An individual is not required to apply for an RFID enabled cross border travel document. If an individual does obtain an RFID enabled card, the individual may still choose to decline to submit the RFID enabled card for automated reading in the dedicated crossing lane. In the event that the individual chooses to not use the RFID enabled card, the individual will still be allowed to cross into the United State through regular border crossing lanes and the document's MRZ will be read. The individual will always be required to provide information before being admitted into the United States. Once fully implemented under WHTI, individuals crossing the border will be required to present a passport, RFID enabled passport card, EDL, other RFID enabled and WHTI compliant travel document or a WHTI compliant travel document without RFID as a means of providing proper identification. Specifics about the Passport Card and Mexican Border Crossing Card are currently being developed. Likewise, various States are developing the particulars of their respective EDL programs. In addition, the DHS will be working with Native American Tribes to develop the parameters for issuing an RFID enabled card.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Participation in trusted traveler programs and certain other programs that will utilize RFID enabled travel documents, such as state or provincial EDL programs, will be voluntary. However, once an individual has consented to the terms of the program and obtained an RFID enabled travel document, the individual no longer has the right to consent to how his or her application information is used if the individual presents the RFID enabled travel document for purposes of crossing the border, as long as it is used in a manner consistent with the described terms. The CBP trusted traveler programs are voluntary. Individuals are informed of the uses of the enrollment/application information, as part of the terms of the program, and consent to the use of the information at the time they apply for the programs. In the future, the DoS Passport Card and Mexican Border Crossing Card, EDL, and Native American RFID cross border travel documents will permit a similar right to consent as part of the initial decision to obtain the card, but having once obtained the card, an individual is presumed to consent to any uses of the information that are consistent with the initial terms.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

As part of the DHS enrollment process, individuals are given educational information on RFID technology, including how to safeguard the RFID card and the RFID number, including to only carry the cards when traveling and to keep the cards in secure location. With non-DHS issued documents, DHS/CBP will recommend that similar educational information is provided to the individual. Depending on the nature of the document, using it only to cross the border, may not be an option.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

To gain access to government-held information stored in GES, trusted travelers may request information about their records through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a (d). Similarly, information pertaining to a traveler's border crossing may be obtained from BCIS in the same fashion.

TECS is a law enforcement information system that is exempt from the access provisions of the Privacy Act; access to records maintained in TECS is available through the FOIA exclusively. Access to information in the database maintained by DoS for the passport card is determined by the system notices and regulations of DoS. Likewise, access to State DMV information for the EDL and Native American Tribal databases for the responsive information maintained by those respective legal authorities is determined by their governing authorities.

7.2 What are the procedures for correcting erroneous information?

Individuals in CBP's trusted traveler program who believe information in GES is incorrect should contact, in writing, CBP's Customer Service Center, Office of Public Affairs, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, DC 20229, Fax: 202-344-2791. The letter to CBP's Customer Satisfaction Unit should explain which information is erroneous and set forth the correct information.

Procedures for the correction of erroneous data that is detected by the CBP Officer during interview, inspection, or investigation are documented within the TECS User Guide. In general, the procedures call for the update of information in the TECS "subject" record and will require supervisory approval. All such correction transactions are logged by TECS and attributed to the authorized user performing the correction. This includes any required supervisory approval.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous PNR data stored in ATS and other data stored in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Procedures for correcting information for other participants, including DoS, States and Tribal governments, will be defined by the authorities governing those entities.

7.3 How are individuals notified of the procedures for correcting their information?

Notification of correction procedures are provided to individual enrolling in CBP's trusted traveler program during the enrollment process and again through this Privacy Impact Assessment, see above.

No individual notification of procedures for correcting TECS records is currently provided. TECS contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notification sent to travelers that they are or have been the subject of a law enforcement investigation would undermine the performance of the law enforcement mission of CBP. However, inasmuch as mistakes in TECS may exist, requests for redress should be directed to CBP's Customer Satisfaction Unit (see section 7.2. above).

Other participants, including DoS, States and Tribal governments, should provide notice to individuals, during the enrollment process, regarding correction procedures, as defined by the authorities governing those entities.

7.4 If no redress is provided, are alternatives available?

Travelers seeking redress for any issue related to the CBP's trusted traveler program or CBP's collection of RFID from a non-DHS issuer in the RFID border crossing process, may apply online to the DHS Traveler Redress Inquiry Program (DHS-TRIP). DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs--like airports and train stations—or crossing U.S. borders

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals seeking redress may apply online through DHS-TRIP, a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

Internal to DHS, CBP Officers will have access to the RFID identifiers as part of the border crossing clearance process at ports of entry equipped with vicinity RFID readers. Other DHS organizations may access information contained in back-end systems, based on an articulated need to know in the performance of official DHS responsibilities. External to DHS,

the governments of Canada and Mexico have access to portions of the trusted traveler program information. The Canadian government can access RFID identifiers within the trusted traveler program while the Mexican government only has access to whether the particular card being used is valid or not valid.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors have limited access to the RFID identifiers stored in GES. Contractors may also have access to biographical information maintained in BCIS and TECS. Contractors with access to BCIS and TECS must have the requisite need-to-know and access to GES before accessing any RFID identifier information from GES. The RFID number is not maintained in TECS.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. GES, BCIS, and TECS use roles to govern user access. Users are assigned to system roles based on a demonstration of "need to know" which is documented in the user's application for access. Access to TECS and BCIS are authorized by the TECS Program Manager and enabled via a TECS User Profile that is generated and entered in TECS by the TECS Security Administrator.

8.4 What procedures are in place to determine which users may access the system and are they documented?

To gain access to CBP information systems, a user must have a need to know, must clear the applicable background check, and complete annual privacy training. A supervisor submits the request to the CBP Office of Information Technology (OIT) indicating the individual has a need to know for official purpose. OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new user account. User accounts are reviewed periodically to ensure that these standards are maintained.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Every six months users must request and immediate supervisors must reauthorize access to BCIS and TECS. Reauthorization is dependent upon a user continuing to be assigned to mission role requiring BCIS and TECS access and the absence of any derogatory information relating to past access.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

BCIS and TECS maintain audit trails or logs for the purpose of reviewing user activity. BCIS and TECS actively prevent access to information for which a user lacks authorization, as defined by the user's role in the system, location of duty station, or job position. Multiple attempts to access information without proper authorization will cause BCIS and TECS to automatically suspend access. Misuse of BCIS and TECS data can subject a user to disciplinary actions in accordance with the CBP Code of Conduct, including being removed from an officer position.

All information provided to CBP by participants in the RFID border crossing program will be protected in accordance with all applicable laws. Information Security requirements as specified in CBP HB 1400-05C, DHS 4300A Sensitive Systems Handbook, as well as applicable NIST guidance, is applied to sensitive data such as Passport data. In addition to information security best practices, all personnel including CBP officers making inquiries into the database, have had a full field background investigation and are given information on a "need-to-know" basis only. Procedural and physical safeguards are also utilized such as accountability and receipt records, audit trails, armed guards patrolling the area, restricted access with alarm protection systems, special communications security, fencing, etc. are also employed.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

The CBP personnel using these systems are required to complete annual training in privacy awareness. The training presents Privacy Act responsibilities and the CBP's policy with regard to the security, sharing and safeguarding of both official information and PII. CBP personnel who do not take the required training will lose access to all computer systems – systems which are integral to the duties of a CBP Officer. Other government users with access the RFID border crossing information will meet the same standards.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. The date of last Certification and Accreditation for GES was May 26, 2006. The date of the last Certification and Accreditation for TECS was January 3, 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

CBP shares the information with Canada as part of joint US-Canadian trusted traveler programs. Information shared with Mexico is limited to travel card status (valid/not-valid). This program status is shared directly relating to whether the cardholder is a member of the program. Specific application information is not shared. As noted earlier, Information related to the DoS passport card and Border Crossing Card, EDL or other RFID enabled travel document may be shared for law enforcement purposes with federal, state, local, tribal, and foreign law enforcement agencies.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

RFID enabled cards and readers/scanners are purchased from commercial vendors. The GES, BCIS, and TECS were built from the ground up. Please consult DoS, the States, the respective Native American Tribes, and CBSA for the source of the system databases.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

RFID technology assists CBP in processing travelers with RFID enabled documents who are crossing the border. RFID-enabled cards are used to trigger retrieval of PII from secured back-end systems that pre-position traveler information on the computer screens of CBP Officers to expedite the clearance process for individual trusted travelers. Only the unique RFID identifier is stored on the RFID tag. All other electronic PII related to the traveler is stored in secured computer systems and networks. Travelers are educated regarding the use of RFID technology and methods to safeguard the RFID card. In addition, the border crossing environment is physically controlled by CBP, whose Officers and the physical layout of the port area serve to prevent unauthorized access to or use of the RFID identifiers.

The system has been modified to collect the Tag ID of the RFID chip as part of the transmission so that any attempt to “clone” the RFID number may be defeated automatically through immediate and direct cross reference between the RFID number and the Tag ID number. Cloning is the illegitimate duplication of an RFID enabled card’s tag data, with the primary intent being the theft of the original card holder’s identity. Because any Gen 2 reader can read any Gen 2 card, cloning of cards is a very possible risk. A person with sufficient technical knowledge and a mobile RFID interrogator could read a card and duplicate the stored data value

to another card. In WHTI and associated EDL programs, this risk is somewhat mitigated. All cards will have visible security measures (holograms, micro-text, etc.) on the card itself, so a properly cloned card would also have to mimic intricate security details. RFID scans are accompanied by an inspection of personal information retrieved from CBP's systems. If the retrieved information (photo, DOB, etc.) does not match the person presenting the card, the card is immediately flagged as counterfeit. Even with these mitigations, the risk of cloning RFID enabled cards and an imposter with similar physical features gaining illegal entry into the U.S., while unlikely, is real. Fortunately, there is a powerful tool that can be used to remove the risk of cloning. This tool is the Tag Identifier, or TID. The TID is available on all Gen 2 RFID tags.

9.3 What design choices were made to enhance privacy?

To provide increased privacy protection, CBP is limiting the information transmitted wirelessly via RFID to a number generated by the issuing authority of the RFID enabled card itself. This number is not derived in any way from personally identifiable information related to the traveler. All personally identifiable information is stored and used in controlled computer systems and networks and is not transmitted wirelessly. Also, the header information in the RFID number that identifies the issuer of the card, has been modified to be a brief numeric representation that the back-end system may interpret by reference to an information table as part of the system.

For trusted traveler programs and all border crossing information collections, CBP chose to restrict the range of its vicinity readers to around fifteen feet so that the read operation would occur within the physical perimeter of the CBP controlled space at the border. NEXUS/SENTRI/FAST and the proposed DoS passport card utilize vicinity tags that are limited by the read range to what is considered 'medium range' by industry standards (around 15ft). Additionally, the RFID enabled cards only transmit when activated by a reader. It is intended that the EDL and other RFID capable ID cards be designed similarly.

Conclusion

DHS, DoS, and States and other entities collect PII from travelers during the enrollment/application process for current or anticipated RFID enabled travel documents. This PII is stored in secured computer systems and is associated with a unique RFID identifier stored in a card the traveler presents during the border crossing process. In order to expedite processing, this unique RFID identifier is transmitted wirelessly from the individual's RFID enabled card to an RFID reader which triggers the CBP computer systems to retrieve the PII stored in secured back-end systems and pre-position the PII associated with that traveler corresponding to the unique RFID identifier. This automated process enables the CBP Officer to quickly compare the information presented on the computer screen with the information on the travel card and the

traveler, and thus enhance security and complete the clearance process faster than if the enrollment information were not available. No personally identifiable information is transmitted via RFID, and the traveler is fully informed of the methods for transmitting and using this information as part of the enrollment process for RFID enabled travel documents.

Responsible Officials

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of International Trade, Regulations and Rulings, Customs and Border Protection, (202) 572-8790.

Colleen Manaher, Director, Western Hemisphere Travel Initiative, Program Management Office, Office of Field Operations, Customs and Border Protection, (202) 344-3003.

Approval Signature Page

Original signed and on file with DHS Privacy Office.

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security