Privacy Impact Assessment
for the

Western Hemisphere Travel Initiative

Land and Sea Rule

August 9, 2007

Rulemaking Contact Point
Colleen M. Manaher
Director, WHTI Program Office
U.S. Customs and Border Protection
(202) 344-3003

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

Abstract

The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP), in conjunction with the Bureau of Consular Affairs at the Department of State (DOS), have published a notice of proposed rulemaking to notify the public of how they intend to implement the Western Hemisphere Travel Initiative (WHTI) for sea and land ports-of entry. The proposed rule, would remove the current regulatory exceptions to the passport requirement provided under sections 212(d)(4)(B) and 215(b) of the Immigration and Nationality Act (INA). The DHS Privacy Office is conducting a Privacy Impact Assessment (PIA) of the proposed rule under the authority of Subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which calls for the DHS Chief Privacy Officer to conduct "a privacy impact assessment of proposed rules of the Department." This analysis reflects the framework of the Privacy Office's Fair Information Principles: Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

Introduction

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, provides that upon full implementation, generally U.S. citizens and nonimmigrant aliens may enter the United States only with passports or such alternative documents as the Secretary of Homeland Security designates as satisfactorily establishing identity and citizenship. The notice of proposed rulemaking (NPRM) is the second phase of a joint DHS and DOS plan, known as WHTI, to implement these new requirements at sea and land ports-of-entry.

Generally, individuals entering the United States from foreign points-of-departure are required to show a valid passport. Sections 212(d)(4)(B) and 215(b) of the INA, however, has provided authority for a waiver of the passport requirement, which has been exercised to exempt U.S. citizens and nonimmigrant aliens from Canada, Bermuda, and, in certain circumstances, Mexico when arriving at the United States from points-of-departure within the Western Hemisphere. Congress, by statute, has provided that these exceptions must be ended with the designation of acceptable alternative documents. The proposed rule, which is the second phase of WHTI implementation, would designate alternative documents and remove this exception for sea and land points-of-entry.

The first phase, for air ports-of-entry, was implemented through a final rule issued on November 24, 2006. (*See* 71 FR 68411) DHS conducted a PIA in conjunction with the publication of the notice of proposed rulemaking for the first phase and updated it upon the issuance of the WHTI Air final rule. Both PIAs are available at the Privacy Office website, www.dhs.gov/privacy.

This NPRM proposes the specific documents that U.S. citizens and nonimmigrant aliens from Canada, Bermuda, and Mexico would be required to present when entering the United States at sea and land ports-of-entry from countries in the Western Hemisphere. DHS and DOS expect the date of full WHTI implementation to be in the summer of 2008. The precise implementation date will be published in the Final Rule or will separately be published, with at least 60 days notice, in the Federal Register.

The NPRM also provides the Secretary of DHS with the authority to designate other acceptable forms of identification in the future. Like the air rule, this proposed rule removes most of the exceptions to

the passport requirement that were granted under the authority of INA sections 212(d)(4)(B) and 215(b).

With some limited exceptions, the proposed rule would require U.S. citizens who wish to enter the United States at a sea or land port-of-entry to present either (1) a U.S. passport book, (2) a U.S. passport card, (3) a valid trusted traveler card issued by DHS (i.e., NEXUS, FAST, or SENTRI programs), (4) a valid Merchant Mariner Document when used in conjunction with official maritime business, or (5) a valid U.S. military identification card when traveling on official orders. Canadian citizens could show either a Canadian passport or a valid trusted traveler program card issued by DHS. Citizens of Bermuda would need to show a passport to apply for admission to the United States. The NPRM also provides for the possibility of other alternative documents such as enhanced drivers licenses issued pursuant to a pilot program or Canadian government documents other than passports.

Mexican citizens would either need to show a Mexican passport with a visa or a valid Border Crossing Card issued by DOS, as is the practice today. The implementation of this rule would foreclose a minor exception to this requirement, allowing entry without a passport or Border Crossing Card for those who enter the United States from Mexico solely to apply for a Mexican passport or other 'official Mexican document' at a Mexican consulate in the United States located directly adjacent to a land port-of-entry.

WHTI does not create a collection of new data elements by DHS; rather it would permit collection of the same information from additional categories of individuals. Similar to the requirement that individuals present a passport upon arrival from a point-of-origin outside the Western Hemisphere, WHTI will now require the same information collection for points-of-origin within the Western Hemisphere by DHS. This change will enable CBP to screen most individuals arriving from foreign travel points to the United States, to identify suspected or actual terrorists or individuals with affiliations to terrorist organizations, individuals who have active warrants for criminal activity, and individuals who are currently inadmissible or have been previously deported from the United States or otherwise identified as potential security risks or raise law enforcement concerns. The standardized and tamper resistant documents proposed in this rule will reduce the number of fraudulent documents presented at the border, and provide further protection against identity theft. In addition to enhancing security, WHTI will expedite travel within the Western Hemisphere by standardizing the documentation presented to CBP at the border and facilitating the inspection of travelers.

CBP is the agency responsible for reviewing and collecting passport information from travelers entering the United States, including travelers from countries within the Western Hemisphere. This is consistent with CBP's overall border security and enforcement missions. The passport data will be collected from individuals at CBP ports-of-entry and stored in CBP's Treasury Enforcement Communications System (TECS).

DHS conducts Privacy Impact Assessments on programs, proposed rules, and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that WHTI land and sea NPRM is a proposed rule rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of the proposed rule as it relates to the Principles of Fair Information Practices.

This PIA will be updated when the final rule is published, and when necessary thereafter.

Fair Information Principles

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information. These concepts are known as the Fair Information Principles (FIPs). The FIPs impose duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

As such, the DHS Privacy Office has developed the FIPs that underlie the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The DHS FIPs, outlined below, account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

1. Principle of Transparency

DHS implements the principle of transparency by informing individuals about what personally identifiable information DHS collects, maintains, uses, and disseminates. DHS provides transparency by publishing PIAs, Systems of Records Notices (SORNs), and with other means, as appropriate.

This PIA describes the privacy implications of the proposed rule. Together with the PIAs issued in support of the WHTI air rule, this PIA provides the public with an accounting of the anticipated collection, maintenance, use, and dissemination of personally identifiable information contemplated by DHS under the Western Hemisphere Travel Initiative.

PIAs for the NPRM implementing the WHTI requirements for air travel (71 FR 68411) are available at www.dhs.gov/privacy.

Presently, CBP collects and stores passport information from all travelers required to provide such information under the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA). CBP maintains this data in the Treasury Enforcement Communications System (TECS). The SORN for TECS is published at 66 FR 53029.

Information collected by CBP for the trusted traveler programs utilized by WHTI (NEXUS, FAST, and SENTRI) is described in a SORN for the Global Enrollment System, published at 71 FR 20708. The SORN covering the DHS Traveler Redress Program (TRIP), which will allow travelers to submit redress requests, is published at 72 FR 2294. DOS published an NPRM, 71 FR 60928, regarding the creation of the passport card, one of the options expected to be available to U.S. citizens to gain entry to the United States from certain points-of-departure in the Western Hemisphere under WHTI. The passport card NPRM describes the anticipated use of radio frequency identification (RFID) on the passport card, which is currently under development. At the border, CBP will employ vicinity RFID readers to access the information (a unique numerical identifier) stored on the passport card. Because there are privacy implications attendant with the use of RFID and vicinity RFID in particular, DHS will issue a subsequent PIA discussing all the uses of RFID by CBP, including the use of RFID on the passport card in support of the WHTI program implementation.

Additionally, to enhance transparency, DHS and DOS have instituted an extensive public information campaign, reaching out to border communities and travel industry professionals. CBP

maintains a website (www.cbp.gov/xp/travel/vacation/kbyg/) to provide additional information to travelers about what documentation is required when traveling outside the United States.

2. Principle of Individual Participation

DHS must, to the extent possible and practical, collect information directly from the individual, as this practice increases the likelihood that the information will be more accurate. Further, at the time of collection, notice will be given to the individual on how the program provides for access, correction, and redress, under section (e)(3) of the Privacy Act of 1974, 5 U.S.C. 552a, as amended.

Information, whether on a passport or trusted traveler card, will be collected directly from United States citizens and nonimmigrant aliens from Canada, Bermuda and Mexico entering the United States at sea and land ports-of-entry from Western Hemisphere countries. This information is already collected from all other persons traveling to or from the United States, and no change to that practice is being made.

Individuals have no opportunity to consent to specific uses of their information for any lawful purpose, including border and immigration management, national security, and law enforcement, consistent with current practice. The proposed rule does not impact this practice.

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 central gateway for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – such as airports and train stations or crossing U.S. land and sea borders. Through TRIP, a traveler can correct erroneous data stored in DHS databases. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or through www.dhs.gov/trip.

3. Principle of Purpose Specification

In order to satisfy this principle, DHS must articulate with specificity the purpose of the program, tying this purpose to the underlying mission of the organization and its enabling authority.

Pursuant to the ATSA and the EBSA, the collection of data off the traveler's passport, or other designated document or combination of documents, is mandatory for law enforcement and national security purposes. While the INA contained a waiver for this requirement in limited circumstances, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) Pub.L. 108-458, 118 Stat. 3638, directs the Secretary of Homeland Security, in consultation with the Secretary of State, to develop and implement a plan requiring passports or other designated document or combination of documents from United States citizens and nonimmigrant aliens for whom the passport requirement was formerly waived.

The goal of the collection is to screen all passengers arriving from foreign travel points to the United States to identify suspected or actual terrorists or individuals with affiliations to terrorist organizations, individuals who have active warrants for criminal activity, individuals who are currently inadmissible or have been previously deported from the United States or have been otherwise identified as potential security risks or raise law enforcement concerns. WHTI is intended to enhance security efforts at our Nation's borders and expedite travel within the Western Hemisphere by reducing the number of different forms of identification and employing more readily verifiable forms of identification.

4. Principle of Minimization

DHS must ensure that personally identifiable information must be directly relevant and necessary to accomplish the specific purposes of the program; and only retained for as long as necessary and relevant to fulfill the specified purposes.

Under the WHTI, information to be collected from United States citizens and most nonimmigrant aliens from Canada, Bermuda, and Mexico entering the United States at sea and land ports-of-entry will consist of data located within each traveler's individual passport as well as related travel itinerary information. This information will include:

Travel document (e.g. Passport, Trusted Traveler Card, or other acceptable document)

Passport Issuance Country

Travel document/Passport Number

Alien Registration Number (if applicable)

Name of Traveler

Date of Birth

Nationality of Traveler

Date of Travel Arrival

Time

Conveyance of Travel

Foreign Place of Departure

Domestic Place of Arrival

This information is already collected from all other travelers not subject to the passport exemption. There are a number of U.S. and Canadian citizens, however, who make numerous land border crossings on a daily basis and from whom this particular set of PII is not collected. Under this proposed rule, CBP will collect the listed PII relating to many millions more border crossings. The collection of this additional information, however, is no more than is necessary to satisfy the requirements of IRTPA and implement WHTI.

5. Principle of Use Limitation

Implementing this fair information principle requires DHS to use and share personally identifiable information only for the purposes for which DHS collected the information and for which the individual received notice.

No new uses of information are contemplated by the sea and land phase of the implementation of WHTI. The goal of the information collection is to screen all travelers arriving from foreign travel points to the United States to identify suspected or actual terrorists or individuals with affiliations to terrorist organizations, individuals who have active warrants for criminal activity, individuals who are currently

inadmissible or have been previously deported from the United States, or who have been otherwise identified as potential security risks or raise law enforcement concerns. WHTI is intended to enhance security efforts at our Nation's borders and expedite the travel within the Western Hemisphere by reducing the number of different forms of identification and employing more readily verifiable forms of identification.

The land and sea proposed rule does not envision new instances of information sharing. Consistent with the "routine uses" described in the TECS SORN, the information collected by CBP may be shared with all component agencies within DHS and with federal, state, local, tribal and foreign law enforcement agencies on a specific need to know basis that is consistent with the component's or agency's mission. The sharing with external agencies includes every law enforcement agency in the federal government as well as those federal agencies mandated to ensure compliance with laws or regulations pertaining to entry or importation into the U.S., each of the 50 states, the District of Columbia, U.S. insular possessions and territories, and a majority of foreign nations with whom the U.S. maintains diplomatic relations.

6. Principle of Data Quality and Integrity

To satisfy this principle, DHS must ensure that personally identifiable information is accurate, compete, and kept up-to-date. This proposed rule relies in part upon the data quality and integrity requirements within the underlying systems.

The principle of data quality is promoted when the government collects information directly from the individual. This is the case with WHTI. Information on the passport, passport card, Border Crossing Card, Merchant Mariner Document, U.S. Military Identification Card, trusted traveler identification, or other document accepted pursuant to this rule will be drawn from information provided to the government directly from the individual. If an identity document is returned to a traveler at the time of issuance with inaccurate information, he or she will have an opportunity to inspect it and have it corrected. At the border, individuals will personally present their acceptable documents to CBP.

The redress processes further enhance this principle. Travelers with discrepancies will have several opportunities to resolve data quality issues. The first will occur in real time at the border during the interaction with CBP. If the traveler still is not satisfied that their information is correct, he may take advantage of the DHS TRIP program.

The tamper resistant qualities of passports, passport cards, Border Crossing Cards, Merchant Mariner Documents, U.S. Military Identification Cards, and trusted traveler cards, as well as the secure issuance processes associated with these documents, also enhance data integrity. If cards may not be altered or forged easily, the government and traveler may have confidence that the information presented is accurate.

7. Principle of Security

DHS must protect personally identifiable information through reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.

The proposed rule relies upon the security of the TECS system underlying the implementation of

WHTI. This system successfully underwent the DHS Certification and Accreditation (C&A) process, and a Security Risk Assessment was completed in compliance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) policy, and guidance provided by the National Institute of Standards and Technology (NIST).

This system actively prevents access to information for which a user lacks authorization, as defined by the user's role in the system, location of duty station, and/or job position. Multiple attempts to access information without proper authorization will cause the system to automatically suspend a user's access. Any misuse of data collected may result in appropriate disciplinary action in accordance with the CBP Code of Conduct, which can include a CBP Officer being removed from his or her position.

DHS acknowledges that the "value" of hacking into a system with personally identifiable information increases as more records are added. Therefore, the TECS system becomes marginally more attractive to willful unauthorized access due to the addition of records relating to U.S. citizens and nonimmigrant travelers, and legal permanent residents. Notwithstanding this fact, the security precautions already in place are sufficient to protect against the added interest unauthorized users would have in the system due to the increase in records.

DHS and DOS are proposing to use a machine readable zone and vicinity RFID to facilitate the inspection of travelers at the border. The security for these facilitative technologies will be the subject of other Privacy Impact Assessments, including one to deal specifically with CBP's uses.

8. Principle of Accountability and Auditing

To satisfy this principle, DHS must develop mechanisms to ensure ongoing compliance with these principles and with the specifics of programs as described in the privacy documentation.

This proposed rule relies upon the accountability and auditing requirements of the underlying systems. These systems maintain audit trails and logs for the purpose of reviewing user activity. On a periodic basis, system access and use are reviewed by the process owner to ensure that only appropriate individuals have access to the system. Additionally, CBP's Office of Internal Affairs conducts periodic reviews of the system in order to ensure that the system is being used in accordance with DHS and CBP policies.

Conclusion

DHS has minimized the impact of the proposed rule covering entries to the United States at sea and land ports-of-entries by U.S. citizens, and nonimmigrant travelers who are citizens of Canada, Bermuda, and Mexico, from points-of-origin within the Western Hemisphere, through the mitigation strategies discussed in this PIA. Passports, and the attendant collection of information on them at the border, are already required for all persons traveling from points of departure outside the Western Hemisphere, and for all travelers to the United States, other than those from countries other than Canada, Bermuda and the United States regardless of their departure point. WHTI removes a limited exemption to the passport requirements. In phase one, the exemption was removed at air ports-of-entry. During the second phase, the NPRM proposes to remove the passport exemption for sea and land ports-of-entry. While information will be collected from a larger class of individuals as a result, the processes for doing so are well

established, applicable PIAs and SORNs are in place, and implementation includes affirmative steps to preserve the FIPs.

Responsible Officials

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

Colleen M. Manaher, Director, WHTI Program Office, Office of Field Operations, U.S. Customs and Border Protection, (202) 344-3003.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security