Privacy Impact Assessment
for the

Western Hemisphere Travel Initiative

WHTI

August 11, 2006

Contact Point
John P. Wagner
Director, Passenger Automation Programs
US Customs and Border Protection
(202) 344-2118

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Bureau of Customs and Border Protection, Department of Homeland Security, in conjunction with the Bureau of Consular Affairs, Department of State, is publishing a notice of proposed rule making to implement the Western Hemisphere Travel Initiative (WHTI). The air/sea requirements of WHTI are the first phase in the implementation of new passport requirements for certain travelers to, and from, the United States as defined in the Intelligence Reform and Terrorism Prevention Act of 2004. WHTI will expand the group from which passport and travel information will be collected from affected travelers. The purpose of collecting this data is to screen passengers arriving from foreign travel points, to the United States to discover travelers that are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, have active warrants for criminal activity, are currently inadmissible or have been previously deported from the United States or may be identified as potential security risks or raise law enforcement concerns. WHTI is intended to enhance security efforts at our Nation's borders, and as well as to expedite the movement of legitimate travel within the Western Hemisphere.

Introduction

Current regulations permit United States citizens and many nonimmigrant aliens from Canada, Mexico, and Bermuda to enter the United States without requiring the use of a passport when traveling within the Western Hemisphere. United States citizens must satisfy the CBP officer of his or her United States citizenship by providing proof of nationality (*e.g.*, birth certificate), and government-issued photo identification (*e.g.*, a driver's license) when arriving from within the Western Hemisphere. Nonimmigrant aliens from Canada and Bermuda must provide adequate evidence of citizenship and identity. Mexican citizens arriving in the United States at ports-of-entry who possess a Form DSP-150, B-1/B-2 Visa and Border Crossing Card (BCC) are currently admitted without presenting a valid passport if they are coming from contiguous territory.

Pursuant to section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) Pub.L. 108-458, 118 Stat. 3638, by January 1, 2008 Department of State (DOS) and Department of Homeland Security (DHS) must develop and implement a plan to require a passport or as yet to be determined alternatives as the Secretary of Homeland Security may designate as denoting identity and citizenship from US citizens and aliens previously exempted from the passport requirement under INA Section 212(d)(4)(B). Accordingly, in order to comply with its congressional mandate the Department of Homeland Security, Bureau of Customs and Border Protection and the Department of State, Bureau of Consular Affairs are issuing a Notice of Proposed Rulemaking (NPRM) to establish the first phase of the Western Hemisphere Travel Initiative program ("WHTI") which would require United States citizens and nonimmigrant aliens from Canada, Bermuda and Mexico entering the United States at air ports-of-entry and most sea ports-of-entry, with certain limited exceptions, to present a valid passport.

This passport requirement would apply to most air and sea travel, including commercial air travel and commercial sea travel (including cruise ships). However, the WHTI also proposed to designate two documents, in addition to the passport, as sufficient to denote identity and citizenship under section 7209, and acceptable for air and sea travel. The first document is the Merchant Mariner Document (MMD) or "z-card" issued by the United States Coast Guard (Coast Guard) to Merchant Mariners when used on official business. The second document is the NEXUS Air card when used with a NEXUS Air kiosk. Lawful Permanent Residents will continue to retain their exemption from the requirement to present a passport in accordance with the provisions of section 211 of the Immigration and Naturalization Act that provide for

presentation of a valid Alien Registration Card as proof of identity. The first phase of WHTI will not apply to pleasure vessels used exclusively for pleasure and which are not for the transportation of persons or property for compensation or hire, or to travel by ferry. Finally, this phase of WHTI will not address United States citizen members of the Armed Forces on active duty.

WHTI does not create a collection of new data elements, but rather 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 permit the same information collection for points of origin within the Western Hemisphere. This change will enable CBP to screen most passengers arriving from foreign travel points to the United States, to discover travelers that are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, have active warrants for criminal activity, are currently inadmissible or have been previously deported from the United States or otherwise may be identified as potential security risks or raise law enforcement concerns. It removes the exceptions to passport use that were available under the Immigration and Nationality Act ("INA") sections 212(d)(4)(B) and 215(b).

CBP is the agency responsible for reviewing and collecting passport information from travelers entering the United States, including 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 Border Crossing Information System ("BCIS") database, which is a component of the Treasury Enforcement Communications System ("TECS").

This Privacy Impact Assessment will be updated, as necessary when the NPRM is final and at a later date to address covered individuals entering or re-entering the United States through land borders.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

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 air ports-of-entry and most sea ports-of-entry will consist of data located within each traveler's individual passport as well as related travel itinerary information (e.g. arrival time, conveyance, foreign place of departure). This information will include:

Travel document/Passport Issuance Country
Travel document/Passport Number (applicable MMD, NEXUS Air Card Number, or Alien Registration)
Name of Traveler, i.e. passport holder
Date of Birth
Nationality of Traveler
Date of Travel
Arrival Time
Conveyance of Travel
Foreign Place of Departure
Domestic Place of Arrival

This information was not previously collected from some of these individuals when they entered the US from within the Western Hemisphere. In those cases where the Merchant Mariner Document, Nexus Air Card, or identification as a Legal Permanent Resident is presented as an alternative to the passport, the same information will be collected from these documents and the electronic files that they reference.

1.2 From whom is information collected?

The information will be collected directly from United States citizens and certain nonimmigrant aliens from Canada, Bermuda and Mexico entering the United States at air and sea ports of entry from Western Hemisphere countries other than Cuba. 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.

Section 7209 does not apply to Lawful Permanent Residents, who will continue to be able to enter the United States upon presentation of a valid Form I-551, Alien Registration Card, or other valid evidence of permanent resident status. (*see*, Section 211(b) of the INA, 8 U.S.C. 1181(b)). It also does not apply to alien members of United States Armed Forces traveling under official orders. (see, Section 284 of INA, 8 U.S.C. 1354). Additionally, section 7209 does not apply to nonimmigrant aliens from anywhere other than Canada, Mexico, or Bermuda. (*see*, section 212(d)(4)(B) of the INA, 8 U.S.C 1182(d)(4)(B) and 8 C.F.R. 212.1). This phase of WHTI will not apply to pleasure vessels used exclusively for pleasure and which are not for the transportation of persons or property for compensation or hire or to travel by ferry.

1.3 Why is the information being collected?

Pursuant to section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) Pub.L. 108-458, 118 Stat. 3638, Congress has mandated the Department of Homeland Security, in consultation with Secretary of State, establish a program 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. Additionally, pursuant to the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), the collection of the traveler's passport data is mandatory for law enforcement and national security purposes.

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

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

The authorities for WHTI include:

- The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub.L. 108-458, 118 Stat. 3638.

- The Immigration and Nationality Act, 8 U.S.C. 1354.
- The Aviation and Transportation Security Act of 2001 (ATSA)
- The Enhanced Border Security and Visa Reform Act of 2002 (EBSA),

CBP presently collects passport data from persons entering the United States, except for U.S. Citizens and Legal Permanent Residents traveling to the U.S. from points of origin within the Western Hemisphere other than Cuba. WHTI removes some exceptions to passport use that were available under the Immigration and Nationality Act ("INA"). Therefore, formerly excepted individuals now will be required to present passports or other designated documentation when they arrive in the United States from points of origin within the Western Hemisphere. This change will expand the group of travelers from whom CBP will collect passport data.

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.

DHS is not collecting additional types of information, but rather is increasing the population from whom the information is collected. Previously, lesser forms of identity, such as a driver's licenses were deemed acceptable for proving identity for these persons when traveling within the Western Hemisphere and this border crossing information was not collected or maintained by CBP.

Accordingly, inasmuch as CBP already collects the subject data from various travelers no additional qualitative privacy risks were identified; however, given the larger population covered, CBP deploys extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of CBP employees. CBP physical security measures include maintaining the information systems and access terminals in controlled space protected by armed individuals. Access to information is restricted by role, responsibility, and geographic location of the employee accessing the information.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

CBP will use the information collected and maintained through the WHTI to carry out its law enforcement, immigration control functions, and national security mission. CBP uses this system to ensure the entry of legitimate travelers, identify, investigate, apprehend and/or remove individuals unlawfully entering the United States, prevent the entry of inadmissible individuals and detect fraud or abuse of United States or other nation's passports.

The information will be cross-referenced with data maintained in CBP's other enforcement databases, notably the Treasury Enforcement Communications System (TECS), and its screening and targeting systems, notably the Automated Targeting System (ATS), to ensure the admissibility of travelers. The data will be shared with enforcement systems, as appropriate, when related to ongoing investigations or operations. A real time image of the data will reside in the ATS as part of the screening functions performed by that

system to assist in the detection of identity theft and fraud (*e.g.*, multiple border transit locations occurring simultaneously employing the same identity).

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

Yes. WHTI will enable CBP to screen all passengers arriving from foreign travel points, to the United States, to discover travelers that are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, have active warrants for criminal activity, are currently inadmissible or have been previously deported from the United States or are subject to other intelligence that may identify them as security risk or raise law enforcement concerns. CBP will use the information collected through WHTI to compare with information collected in law enforcement databases to identify possible matches or patterns of activity for the purpose of assisting future law enforcement efforts.

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

Information collected from travelers under WHTI will be maintained in the Border Crossing Information System (BCIS), which is now part of the Treasury Enforcement Communications System (TECS). The information will be collected by running the machine readable zone (MRZ) of the passport through a scanner-like reader or through the use of other technology like RFID chips in documents like the ePassport so as to minimize human error in inputting information into the system. The information will be verified by CBP Officers checking the passports at time of arrival into the United States. Prior to the issuance of the final rule, a new system of records will be created for the BCIS.

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

As with any collection of personal information, there is a risk of misuse of the information. To mitigate this risk, access to border crossing data will be controlled through passwords and restrictive rules. Users are limited to the roles that define authorized use of the system. Procedural and physical safeguards are utilized such as accountability and receipt records. Management oversight will be in place to ensure appropriate assignment of roles and access to information.

In order to become an authorized user, an officer must have successfully completed privacy training and hold a full field background investigation. Finally, an officer must not only complete the above, but must have a "need-to-know" the information.

Section 3.0
Retention

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

The information collected from traveler's passport documentation and held within the BCIS database is subject to retention requirements established by the National Archives and Records Administration ("NARA") and published in the system of records notices for the databases in which the information is maintained. The information initially collected through BCIS is used for entry screening purposes. Collected data that matches records against which it is being screened will be shared with the TECS database while an individual traveler is clearing primary inspection. A review of the record retention and disposition schedule for both the BCIS and TECS databases is being planned with NARA as part of both the current review and updating of the TECS System of Records Notice and the creation of the BCIS System of Records Notice. It is anticipated that information stored in the BCIS database will be retained for forty years; information stored in the TECS database will be retained for as long as operationally necessary, subject to retention reviews that occur both periodically and each time information is accessed, but in no case will information be retained longer than fifty years past the date of collection.

The collected passport data is also transferred to the Passport Records System at the Department of State. Information stored in the Department of State's passport records systems is subject to retention in accordance with the National Archives and Records Administration's approved record schedule for the Department of State.

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

A review of the record retention and disposition schedule for both the BCIS and TECS databases is being planned with NARA as part of the current review and updating of the TECS system of records notice.

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

Information is required to be retained in BCIS for a period of forty years to permit the cross-referencing and review by CBP analysts of historical data relating to individuals who cross the border. This 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?

The information collected through WHTI may be shared with all component agencies within the Department of Homeland Security on a need to know basis consistent with the component's mission. Access to BCIS and border crossing information within DHS is role based according to the mission of the component and need to know.

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

One of the objectives of sharing data within DHS is to provide the DHS law enforcement community with information from or about suspected or known violators of the law in a timely manner. This objective supports CBP's and DHS law enforcement and counter-terrorism missions. All component agencies of DHS that have a law enforcement need to know, may have access to the relevant border crossing information, that includes passport data collected as part of the WHTI.

4.3 How is the information transmitted or disclosed?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's internal data sharing of the border crossing data is required to comply with statutory requirements for national security and law enforcement systems: access terminals, mainframe processors, and databases are all maintained in DHS controlled space protected by armed guards. Hard copies of information are protected by sealed envelope and shared via official intra-agency courier. All information is kept secure, accurate and controlled. Authorized personnel must possess a mission or job related need and intended use before access may be granted.

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

In order to mitigate the privacy risks of personal information being misused or inappropriately used, the information is shared only with DHS personnel who have established a need to know the information as part of performance of their official employment duties. Internal DHS access to the border crossing 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. Additionally, any individual with access has gone through privacy training.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

The information, as warranted by specific request or Memorandum of Understanding, will be shared on a "need to know" basis with respective Federal, state, local, tribal, and foreign law enforcement agencies. Presently, this 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 Fifty 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.

Information is regularly transferred to the Passport Records System at the Department of State.

5.2 What information is shared and for what purpose?

All information collected from the passport and relevant to the border crossing at the time of entry into the United States is subject to being shared for reasons of admissibility, border security, and general law enforcement purposes.

All relevant passport data is transferred to Passport Records System at Department of State as a means of confirming the identity of the person crossing the border. This confirmation of identity allows CBP to make a more informed decision regarding admissibility and permits the proper association of the act with the individual for the maintenance of historical records.

5.3 How is the information transmitted or disclosed?

The information may be transmitted either electronically or as printed materials to authorized personnel. CBP's external data sharing of the border crossing data is required to comply with statutory requirements for national security and law enforcement systems. All information is kept secure, accurate and controlled. Additionally, Memoranda of Understanding, defining roles and responsibilities, have been executed between CBP and each agency that regularly accesses TECS or BCIS. Lastly, information that is shared with other agencies, Federal, state, local, tribal, or foreign, outside of the context of any MOU requires a written request by the agency specifically identifying the type of information sought and the purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the Chief, Privacy Act Policy and Procedures Branch, Office of Regulations & Rulings, CBP, insofar as the request and use are consistent with the Privacy Act, the published routine uses for TECS and BCIS, and the receiving agency agrees to be restricted from further unauthorized sharing of the information. All three requirements—use consistent with purpose for collection, sharing consistent with a statutory or published routine use, and acceptance of the restriction barring dissemination outside the receiving agency—and the legal responsibility clause for wrongful dissemination contained in the Paperwork Reduction Act (44 U.S.C. section 3510) are stated as conditions pertaining to the receiving agencies acceptance and use of the shared information. These conditions are stated in the written authorization provide to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

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?

Yes, CBP currently has Memoranda of Understanding with various federal law enforcement agencies, within the Departments of Justice, Treasury, State, and Commerce that have access to TECS. These MOUs address the access and use of TECS data by those agencies. With respect to BCIS data, that was formerly maintained as a database within TECS, the access and use of this data will be subject to the same MOU's and rules for sharing.

5.5 How is the shared information secured by the recipient?

Recipients of TECS and BCIS data are required by the terms of their sharing agreement (MOU) to employ the same or similar precautions as CBP in the safeguarding of the TECS and BCIS information that is shared with them.

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 and BCIS information (that is external to CBP) to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in the TECS and BCIS database.

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

When sharing information with third parties, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the interface request and the implications on privacy related concerns are two factors that are included in the both the initial and ongoing authorization, the MOU and Interconnection Security Agreement 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 limitations on use. The Interconnection Security Agreement ("ISA") specifies the data elements, format and interface type to include the operational considerations of the interface. MOU's and ISA's are periodically reviewed and outside entity conformance to use, security and privacy considerations is verified before Certificates to Operate are issued or renewed.

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?

CBP will be issuing a new System of Records Notice, the Border Crossing Information System. It will be created from an existing database within TECS. The System of Records Notice publication for BCIS will be published prior to the final rule. Notice is also provided through the publication of this PIA on the internet, and both the notice of proposed rulemaking concerning the removal of this exemption and the final rule publication in the Federal Register. Additionally, CBP has set up a web site [www.cbp.gov/xp/cgov/travel/vacation/kbyg/] to provide additional information to travelers about what documentation is required when traveling outside the United States.

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

No. Information must be provided pursuant to applicable statutes from all persons traveling to the United States. The only legitimate means of declining to provide the subject information is to choose not to enter or depart to or from the United States.

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?

No, individuals do not have the right to consent to particular uses of the information. Individuals may only choose whether or not to enter the United States.

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

There is a risk that individuals will not know that they are required to provide their passport information and that the regulations have changed. For this purpose, CBP will be providing notice through publications on its website such as "Know before You Go" [www.cbp.gov/xp/cgov/travel/vacation/kbyg/], this PIA, and the several Federal Register publications relating to rule change concerning this regulation. In addition, CBP's Office of Public Affairs, will be coordinating a press roll-out for the new passport requirements in conjunction with the adoption of the new rule.

Section 7.0
Individual Access, Redress and Correction

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

The TECS system of records is exempt from the access provisions of the Privacy Act, as a law enforcement system may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual. (See, the following exemptions claimed in the Privacy Act System of Records Notice for TECS, 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (5) and (8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2)). The BCIS system of records will not claim exemption from access.

Individuals may seek redress regarding information that may be collected pertaining to them in TECS and BCIS by writing or faxing an inquiry to the Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, fax (202) 344–2791. Additionally, Individuals may seek access to their specific information by filing a Freedom of Information Act or Privacy Act request with the Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, fax (202) 344–2791.

7.2 What are the procedures for correcting erroneous information?

CBP has a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems. If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquires should be direct to the Customer Satisfaction Unit at the following address: Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, fax (202) 344–2791. Individuals making inquires should provide as much identifying information as possible regarding themselves, to identify the record(s) at issue. The Customer Satisfaction Unit will respond in writing to each inquiry.

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

The TECS system contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Requests for redress should be directed to CBP's Customer Satisfaction Unit (see section 7.2. above). The BCIS system is not exempt from the amendment provisions of the Privacy Act; therefore, if a traveler believes incorrect or inaccurate information exist inquires may be made to CBP's Customer Satisfaction Unit (see section 7.2 above).

7.4 If no redress is provided, are alternatives available?

Redress is provided.

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.

CBP is currently in the process of modifying the redress and correction mechanism for individuals that need to correct data collected. This effort is part of a DHS effort to develop a "one-stop" redress process for all travelers, irrespective of whether or not the traveler is subject to the procedural rights provided by the Privacy Act of 1974.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Access to the system is granted and limited to a need to know basis. All parties with access to data are required to have full background checks. The universe of persons with access includes, CBP Officers, DHS employees, Federal law enforcement officers, IT specialists, program managers, analysts, and supervisors of these persons.

8.2 Will contractors to DHS have access to the system?

Yes, subject to the same background, training, need-to-know, and confidentiality requirements as employees.

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

Yes. The system, using the existing infrastructure for TECS will assign roles based on the individual's need to know, official duties, agency of employment, and appropriate background investigation and training.

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

In order to gain access to the BCIS information, a user must not only have a need to know, but must also have appropriate background check and completed annual privacy training. A supervisor submits the request to the Office of Information Technology (OIT) at CBP indicating the individual has a need to know for official purposes. 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 a user must request and his or her immediate supervisor must reauthorize access to TECS (and BCIS). Reauthorization is dependent upon a user continuing to be assigned to a mission role requiring TECS (and BCIS) 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?

TECS and BCIS maintain audit trails or logs for the purpose of reviewing user activity. TECS and BCIS 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, and/or job position. Multiple attempts to access information without proper authorization will cause TECS and BCIS to suspend access, automatically. Misuse of TECS and BCIS data can subject a user to discipline in accordance with the CBP Code of Conduct, which can include being removed from an officer's position.

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

All users of the TECS (and BCIS) database are required to complete and pass a bi-annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to TECS and BCIS. This training is regularly updated.

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

Yes, WHTI data, as a component of TECS, is approved through TECS Certification and Accreditation under the National Institute of Standards and Technology. The last certification was in January 3, 2006.

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

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

Section 9.0 Technology

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

The data collected through WHTI is maintained using an existing data module that was formerly part of the Treasury Enforcement Communication System, an established law enforcement and border security database within CBP. The data module is now being identified as the Border Crossing Information System to provide more transparency into CBP's information collection and use processes. CBP previously collected passport information and stored it within the TECS system.

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

The inclusion of formerly exempt individuals from the collection of passport information, as proposed in WHTI, and the proposed storage of this information in TECS prompted the redesignation of that specific database as a separate Privacy Act System of Records: the Border Crossing Information System (BCIS). BCIS permits greater visibility to the traveling public regarding where CBP maintains records of a persons border crossing information and what those records are.

BCIS permits CBP to maintain a historical record of border crossings. Inclusion in BCIS does not indicate a law enforcement record.

9.3 What design choices were made to enhance privacy?

The principle design choice made to enhance privacy with respect to the Western Hemisphere Travel Initiative was to create a separate and distinct System of Records under the Privacy Act to contain the passport information collected and shared under WHTI. The BCIS system of records, while permitting the sharing of requested information with other systems for purposes of verifying the information collected from the traveler, precludes the automatic sharing of all collected information with law enforcement systems. This means that BCIS will share enough information to confirm a match of passport data as a means of verifying identity, but will not exchange information for the purpose of it being retained in the

verifying system. BCIS also creates a separate and distinct location for the retention of information collected upon a person's crossing of the United States border.

Conclusion

The Western Hemisphere Travel Initiative involves the removal of an exception for United States citizens and certain foreign nationals from having to present a passport in connection with Western Hemisphere travel. These individuals must now present a passport (or an alternative identification as previously discussed) when traveling from points of origin both within and outside of the Western Hemisphere. The Western Hemisphere Travel Initiative expands the number of individuals submitting passport information for travel within the Western Hemisphere, but does not involve the collection of any new data elements. Presently, CBP collects and stores passport information from all travelers, required to provide such information pursuant to the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), in the Treasury Enforcement Communications System (TECS) (a System of Records Notice for which is published at 66 FR 53029). By removing the exception for submitting passport information from United States citizens and certain foreign nationals traveling within the Western Hemisphere, DOS and CBP are requiring these individuals to comply with the general requirement to submit passport information when traveling to the United States.

Responsible Officials

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of Regulations and Rulings, Customs and Border Protection, (202) 572-8712.

John Wagner, Director, Passenger Automation Programs, Office of Field Operations, Customs and Border Protection, (202) 344-2118.

Reviewing Official:

Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, (571) 227-3813.