Privacy Impact Assessment
for

CBP Procedures for Processing Travel Documents at the Border

July 2, 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), Department of Homeland Security (DHS), is publishing this Privacy Impact Assessment to give notice of its procedures for recording certain border crossing information and validating the travel documents provided by individuals at air, land, and sea ports of entry who are admitted or paroled into the United States. CBP maintains information regarding persons who are admitted or paroled[1] into the United States, and where applicable exit the United States in accordance with the Privacy Act system of records notices (SORNs) for the Border Crossing Information (BCI) and for the Treasury Enforcement Communications System (TECS), which is being revised and will be republished in the future as TECS (no longer an acronym).

As part of processing travelers at the border, CBP accepts different types of documents for purposes of establishing the identity, citizenship, and admissibility of travelers seeking to enter the United States. CBP populates BCI with certain information provided by or on behalf of persons who are admitted, paroled into, or depart the U.S. In addition the information maintained by BCI regarding such persons may be derived from different DHS systems of records, Department of State systems of records, and the systems of other governmental or tribal authorities (including foreign governments). CBP uses this information to validate the travel documentation provided by or on behalf of the individual, make determinations regarding an individual's admissibility, and ensure compliance with all other U.S. laws enforced by CBP at the border.

This PIA explains the information technology and the information flow between BCI, TECS, and other Privacy Act system of records, including the Non-Federal Entity Data System (NEDS).

Introduction

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. In meeting this mission, CBP is responsible for collecting and reviewing border crossing information regarding persons entering and, where applicable, exiting the United States.

CBP collects the data maintained in the BCI pursuant to the Enhanced Border Security and Visa Reform Act of 2002, Aviation and Transportation Security Act of 2001, Intelligence Reform and Terrorism Prevention Act of 2004, Immigration and Nationality Act, as amended (8 U.S.C. 1185), and Tariff Act of 1930, as amended (including, 19 U.S.C. 66, 1433, 1459, 1485, 1624 and 2071). Most of this information is derived from the travel documents that all individuals present to CBP when entering, and in some instances when departing, the United States. The other information (such as point of entry and date and time of entry) in BCI is maintained by CBP to facilitate and complete the record of that entry or exit.

[1] The parole authority in section 212(d)(5) of the Immigration and Nationality Act allows for aliens who appear not to be qualified for admission to be granted permission for a temporary stay in the United States "on a case-by-case basis for urgent humanitarian reasons or significant public benefit."

CBP will, in some instances collect this information through the physical inspection of the border crossing travel document, including the swiping the machine readable zone (MRZ) of the travel document to retrieve biographical information. Alternatively, where available and appropriate, CBP will use an identifier, such as a Radio Frequency Identification (RFID) number[2], embedded in the travel document to electronically retrieve the traveler's biographic information and validate the traveler's identity, citizenship and admissibility. When necessary, CBP will manually type in the biographic data from the travel document.

Several different SORNs may be applicable when an individual crosses a border, depending on the context of the border crossing. For example, an individual using a Trusted Traveler Program card at the land border will have provided information to CBP as part of registration and acceptance into that program, and this information will be covered by the Global Enrollment System (GES) system of records notice. Another traveler may fly to the United States and the pre-submission of certain information will be covered by the Advance Passenger Information System (APIS) system of records notice. Many of these systems of records were previously covered by the Treasury Enforcement Communications Systems (TECS) SORN, last published in Federal Register on October 18, 2001, 66 FR 53029. This SORN is being revised and will be reissued by DHS and the system will be known simply as TECS (not an acronym, as it was previously).

To provide expanded notice and transparency to the public, DHS and CBP are publishing new Privacy Act System of Records Notices. As part of DHS's ongoing effort to increase transparency regarding the collection of information at the Department, as well as its efforts to specifically review the personally identifiable information (PII) maintained on the TECS information technology platform, DHS and CBP have identified different data sets that call for individual notice so as to provide appropriate routine uses, retention, and exemptions to the Privacy Act.

The following CBP SORNs maintain information regarding a person's crossing at the border and also contribute information that is maintained in the BCI system of records, which is being published in the Federal Register concurrently with this PIA:

- *Global Enroll System (GES)*: This system of records last published, April 21, 2006, 71 FR 20708, collects, maintains, and disseminates information regarding individuals enrolled in one of DHS/CBP's Trusted Traveler Programs. For trusted travelers, CBP reads either the RFID number, from a chip embedded in the travel document, the MRZ on the back of said document, to obtain information to reference the associated biographical data and photo being maintained in GES.
- *Advanced Passenger Information System (APIS)*: This system of records last published August 23, 2007, 72 FR 48349, was previously part of TECS. It covers the required advanced submission of passenger and crew information for certain air and sea carriers and any other forms of passenger transportation, including rail, which is or may subsequently be mandated or provided on a voluntary basis.
- *Non-Federal Entity Data System (NEDS)*: This is a new system of records that is intended to support certain travel documents, such as Enhanced Driver's Licenses, issued by other government authorities, such as states, Canadian provinces or Canadian territories, that

[2] See "Use of Radio Frequency Identification (RFID) Technology for Border Crossings" PIA published on January 22, 2008 on the DHS Privacy Office's web site, www.dhs.gov/privacy under "Privacy Impact Assessments."

agree to provide CBP with a copy of the database storing biographical information and a photograph pertaining to each document holder in advance of the traveler crossing the border. For such travel documents, CBP will use the identifier embedded in the travel document, read the MRZ to retrieve the biographical information and photo pertaining to the travel document from NEDS to assist CBP officers in making admissibility determinations by electronically validating information on those travel documents.

- *TECS*: This system of records last published in Federal Register on October 18, 2001, 66 FR 53029. This SORN is being revised and will be reissued by DHS and the system will be known simply as TECS (not an acronym, as it was previously). It is used for the screening of travelers at primary inspection and maintains data on individuals when an enforcement action has been taken, for example an individual is sent for additional screening, instances involving wants, warrants, or lookouts concerning persons, or instances where law enforcement or intelligence agencies have identified information or contexts that relate to a person.

In addition to the above CBP systems of records, CBP maintains information from other DHS components, such as U.S. Citizenship and Information Services (CIS), and other Federal Agencies, specifically Department of State (DoS), in order to validate the travel documents provided by an individual. So for example, CBP maintains a near real time copy of the Department of State's visa data and US Passport data on the TECS IT platform in order to verify the accuracy of visa and Passport data. The data sets, from this example, are identified such that they follow the Department of State's Privacy Act system of records privacy rules until the individual has crossed the border, and DHS has recorded the information in BCI. Similarly, data obtained from other DHS component or agency systems of records will be used according to a similar practice.

This information is collected in order to validate the documentation provided by the individual, to make determinations regarding an individual's admissibility, to identify security risks to the U.S., to expedite CBP processing of legitimate travelers upon arrival in and prior to departure from the United States, and to ensure compliance with all other U.S. laws enforced by CBP at the border.

Once the individual is legally admitted or paroled into the U.S. by CBP at the United States border or its functional equivalent, a record will be created in BCI. Similarly, as a person complies with the exit requirements for departure from the United States, a record will be created in BCI. For persons denied admission into the U.S. a record of the encounter at the border will be maintained in TECS. For individuals seeking admission to the U.S. by land or sea who present a travel document that requires access to information that may be maintained in NEDS, USCIS system of records, or a DoS system of records, the proper data set will be accessed and the performance of law enforcement queries will be conducted only when the traveler arrives at the border and presents the respective travel document. Disclosure of information in NEDS may also be made consistent with the Privacy Act (5 U.S.C. 552a). Information obtained through APIS will be screened in advance, in accordance with the processes described in that PIA.

At the land border, there are several different data sets that CBP may access to retrieve the biographical data and photograph to validate the use of the individual's travel documents and record that person's lawful crossing of the border:

- From CBP's GES for a Trusted Traveler Program card;
- From the Department of State for Passport cards, Passports, Visas, or Border Crossing Cards;
- From U.S. Citizenship and Immigration Services' (CIS) Central Index System for Permanent Resident Card holders;
- From the NEDS database, information that other government and tribal authorities, such as states, Native American Tribes, Canadian provinces or Canadian territories, agree to provide to CBP for CBP's acceptance of a travel document issued by that entity, such as an Enhanced Driver's License, for purposes of obtaining admission or being paroled into the United States;
- From another government authority that agrees to provide CBP with access to databases maintained by it for purposes of verifying the identity, citizenship and admissibility of individuals bearing travel documents issued by those entities, and ensuring compliance with all other U.S. laws enforced by CBP at the border (e.g., Merchant Mariner Document, U.S. Military Identification Card).

With regard to travel documents issued by entities outside the federal government and pursuant to the Western Hemisphere Travel Initiative (WHTI) requirements, DHS identified two options with regard to electronic verification of the biographic data and photograph of individuals presenting an enhanced identification card, enhanced tribal card, or enhanced driver's license (together referred to as an Enhanced Driver's License (EDL) for the purposes of this document) upon entering the United States at a port of entry. One option requires that a copy of the entire database holding the biographic data and photo be shared by the issuing authority with CBP, so that CBP may access individual records as a traveler chooses to present an EDL upon crossing the border. The second option requires that CBP obtain individual biographic data and photograph from a database maintained by the issuing authority on each occasion when a traveler presents an EDL upon crossing the border. The first option requires CBP to maintain and update a database containing each governmental or tribal entity's entire border crossing travel document data set, whether or not all persons in the database choose to cross the border at any given time. The second option does not require CBP to maintain such a database. Both options only provide information to BCI at the time a person chooses to cross the border using an appropriate border crossing travel document

In consideration of privacy, CBP has limited the sharing of NEDS data to the statutory disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act, and has chosen not to publish any routine uses pursuant to 5 U.S.C. 552a(b)(3). This provides an individual possessing an approved travel document, such as EDL, whose data is shared with CBP prior to crossing the border with a similar level of privacy as the individual whose data is shared at the time of crossing with CBP. In both cases, CBP will access the personally identifiable information associated with a travel document and will create a record in BCI and/or TECS where this information is necessary to verify the identity, citizenship and admissibility of an individual when he or she attempts to enter the United States and to ensure compliance with all other U.S. laws enforced by CBP at the border, or under those circumstances where disclosures are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.

This PIA in large part discusses the BCI and NEDS system of records. Other systems of records are discussed, including GES and TECS. GES has an already published PIA and SORN, and the PIA is being drafted as part of the update to the SORN for TECS.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

Border crossing information that will be collected from all persons crossing the borders of the United States at air and sea ports-of-entry, as well as land border crossings, may include data located within each traveler's individual passport or travel document, as well as related travel itinerary information (e.g., arrival time, type of conveyance, foreign place of departure) listed on required documents; in the case of those arriving via commercial and certain private conveyances, certain information will be supplied by the appropriate company/operator prior to arrival. The following information will be maintained in BCI (upon legal admission or parole into the United States) and/or TECS, as appropriate, and may include, where applicable:

- Travel Document Type (e.g. Passport, Passport Card, Visa, Form I-551 Permanent Resident Card, Trusted Traveler Program Card, or at land/sea borders an acceptable RFID enabled border crossing travel document, such as an Enhanced Drivers License)
- Travel Document Number/Passport Number
- Country or Entity issuing the Travel Document
- Expiration Date of the Travel Document
- Full Name (First, Middle, and Last)
- Date of Birth
- Gender
- Country of Citizenship
- RFID Tag Number(s) (if land/sea border crossing)
- Date of Crossing
- Arrival Time
- Conveyance of Travel, e.g. on an aircraft, vessel, vehicle
- Foreign Place of Departure
- Location of Crossing
- Lane for Clearance Processing
- Secondary Examination Status
- License Plate or VIN number of the conveyance used to enter the United States
- Flight/Voyage number
- Photograph of the Individual, where available

In those cases where a WHTI-compliant document, such as a Merchant Mariner Document or military identification card, is presented as an alternative to the passport, similar information will be collected in BCI from these documents

For expedited processing of certain travel documents, DHS/CBP has set up NEDS which will maintain information on individuals who have signed up for the EDL or other WHTI-compliant document issued by a non-federal entity that agrees to provide CBP with a copy of the data associated with these travel documents. The information maintained in NEDS includes:

- Travel Document Type (e.g. RFID enabled border crossing travel document)
- Travel Document Number/Passport Number
- RFID Tag Number(s)
- Country or Entity issuing the Travel Document
- Expiration Date of the Travel Document
- Full Name (First, Middle, and Last)
- Date of Birth
- Gender
- Country of Citizenship
- Photograph of the Individual, where available

1.2 From whom is information collected?

To the extent available, this information is collected from all persons seeking admission to the United States.

In the case of NEDS, information is collected by CBP from an issuing authority, such as a state Department of Motor Vehicle (DMV) after that information is voluntarily provided to the issuing authority by individuals applying for certain travel documents, such as an EDL, which will facilitate their entry into the United States. Information maintained in GES, APIS, or other Federal databases is collected from the traveling public in accordance with the terms of the PIAs and SORNs published for these systems. (*see* Appendix)

Information maintained in BCI is collected through NEDS, GES, APIS, or TECS (as a result of manual entry of the data or an MRZ read) as part of a person's presentation of their travel document to seek admission to the United States. This information is then screened through TECS prior to CBP's determination of admissibility. At the time that CBP determines that a person is admitted or may be paroled into the United States, the border crossing information pertaining to that person is recorded and maintained in BCI.

1.3 How is the information collected?

With the exceptions of either the manual entry or an MRZ read of data from a travel document, biographic data and, where available, a photo will be collected by either a copy transmission of data from a CBP controlled system or a copy transmission of data from a non-Federal authority controlled system to validate, electronically, the information on the travel document presented for admission. These two methods of transmitting a copy of data from the location, where it is maintained, reflect different approaches to sharing data. One method requires that a copy of the

relevant fields of a database holding the biographic data and photo be shared with and stored by CBP, so that CBP may access the individual records, selectively, as a person chooses to cross the border using the respective travel document. The other method requires that CBP have available transmission lines to obtain, expeditiously, the individual records from the original database holding the biographic data and photo—in this method, only the data pertaining to the person choosing to cross the border using the respective travel document is shared with CBP at the time that admission to the United States is sought. The first method requires CBP to maintain a separate database containing each governmental entity's entire RFID enabled border crossing travel document data set as a separate portion of the database, whether or not all persons in the database are choosing to cross the border at any given time. The latter method does not require CBP to maintain such a database. Both methods only provide information to CBP for screening at the time a person chooses to cross the border using an appropriate RFID/MRZ enabled border crossing travel document.

In the case of either a manual entry of data or an MRZ read data from a travel document, the biographical data pertaining to the traveler is entered into TECS for screening. After CBP has determined to admit or parole the traveler into the United States, the border crossing information, including the traveler's biographical data, is transmitted to BCI. The information may also be recorded in TECS to the extent that some enforcement action may have been taken with respect to that traveler or admission into the U.S. has been denied.

1.4 Why is the information being collected?

Biographical information is collected from all travelers in order to satisfy an inspecting CBP officer of the traveler's identity and citizenship, and to establish whether the traveler is admissible into the United States and to facilitate CBP's enforcement of other U.S. laws at the border.

Border crossing information is also collected as part of the process for screening persons arriving in the United States from, or departing the United States to, foreign travel points. The information is used to discover travelers that are identified as, or suspected of being, terrorists or having affiliations to terrorist organizations, have active warrants for criminal activity, are currently inadmissible or have previously been deported from the United States or have been otherwise identified as potential security risks or raise law enforcement concerns. Collection of this information is intended to enhance security efforts at our Nation's borders, and expedite the movement of legitimate travelers, by enabling CBP to maximize its resources through vetting persons arriving in the United States prior to their physical arrival (or in the case of the land border, immediately prior to inspection by a CBP Officer) in the United States.

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

The authorities for BCI 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. 1185, 1354.
- The Aviation and Transportation Security Act of 2001 (ATSA)
- The Enhanced Border Security and Visa Reform Act of 2002, and
- The Tariff Act of 1930 as amended, 19 U.S.C. 66, 1433, 1459, 1485, 1624, and 2071

CBP collects travel document data from most persons entering, and to some extent departing, the United States, pursuant to the noted authorities under the Immigration and Nationality Act and the Tariff Act of 1930. Under past practice, United States citizens entering and departing the United States from within the Western Hemisphere were permitted to establish identity and citizenship by relying on an oral declaration rather than providing a travel document. The Western Hemisphere Travel Initiative, implementing the statutory mandate of the Intelligence Reform and Terrorism Prevention Act of 2004, will require that all persons entering and departing the United States to present passports or other designated documentation when they arrive in or depart from the United States. This requirement is the subject of a separate PIA regarding the WHTI Final Rule published on March 24, 2008.

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 documents or combination of documents from United States citizens and nonimmigrant aliens for whom the passport requirement was formerly waived. Lastly, the Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 require that the collection of the traveler's passport data be mandatory for law enforcement and national security purposes.

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

With the creation of BCI, CBP is providing additional transparency to its processes for managing information collected that pertains to persons crossing the border. CBP has determined that it would be in the best interest of the public to establish separate systems of records to maintain records on travelers who were lawfully admitted or paroled into the United States and to support the databases shared by other issuing authorities that provide biographical data used to create a border crossing record. CBP is also providing greater access to the information collected from or about the traveler by separating such border crossing information from that information contained in TECS, a system that contains records on individuals who are subject to some enforcement action (including referral to secondary inspection) or who are suspected of violating the law and is exempt from certain provision of the Privacy Act, 5 U.S.C. 552a. CBP does not assert exemptions with respect to individual requests for access to the biographical and biometric information obtained from or about the traveler to the extent it is maintained in BCI.

With the creation of NEDS, CBP will be maintaining additional data necessary for border crossing purposes and only will access that information where this information is necessary to verify the identity, citizenship and admissibility of an individual when he or she attempts to enter the United States and to ensure compliance with all other U.S. laws enforced by CBP at the border, or under those circumstances where disclosures are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act. NEDS information will be provided to CBP by the various issuing authorities pursuant to the terms of separately negotiated Memoranda of Understanding, and CBP's use of this data will be in accordance with the grant of access to the issuing authorities' data and the terms of the NEDS SORN.

Accordingly, inasmuch as CBP already collects the information maintained in BCI from various travelers and those collections are discussed more fully in other Privacy Impact Assessments for the applicable systems in which that data is initially maintained, the additional privacy risk that was identified relates only to the larger population covered. However, CBP deploys extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of CBP employees and, therefore, the expansion of the population from whom data is derived should have no impact upon the level of privacy protections provided.

Given the additional information being provided to CBP by other government authorities and maintained in NEDS, DHS has deployed appropriate security and access controls for such data to mitigate the potential risks associated with its maintenance of this data.

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 in NEDS to support certain travel documents presented at the border denoting citizenship and identity for purposes of determining admissibility into the United States and for purposes of enforcing the laws administered by CBP at the border. This information from NEDS will, upon presentation of the appropriate travel document, be displayed in TECS, for screening, and upon admission or parole into the United States of the person presenting the travel document, a copy of the information will be maintained in BCI along with information pertaining to the time and location of the border crossing. CBP, also, may use the information collected through BCI and TECS to carry out its law enforcement, immigration and border control, and national security missions, as appropriate.

CBP uses these systems to facilitate the entry of legitimate travelers, identify, investigate, apprehend and/or remove individuals unlawfully entering the United States, detect fraud or abuse of United States or other nation's passports, and to otherwise enforce U.S. laws at the border.

The information, presented by a traveler for admission, will be cross-referenced with data maintained in CBP's other enforcement databases, notably the law enforcement data maintained in TECS, and its screening and targeting systems, notably the Automated Targeting System (ATS)

DHS/CBP-006, August 6, 2007, 72 FR 43650, to assist in determining the admissibility of, and security and law enforcement risks posed by travelers. The data will be shared with enforcement systems, as appropriate, when related to enforcement activities, including ongoing investigations or operations. A real time image of TECS data will reside in the ATS as part of the screening functions performed by that system to assist CBP in carrying out its law enforcement functions, including detection of identity theft and fraud (*e.g.*, multiple border transit locations occurring simultaneously employing the same identity).

As part of CBP's implementation of WHTI, CBP may acquire information from various state and Canadian databases, or from other entities such as tribal governments, that agree to provide CBP with a copy of biographical information related to travel documents, such as Enhanced Driver's Licenses, to be accepted by CBP for purposes of entering the United States. These travel documents will utilize RFID technology to transmit an identifying number to CBP RFID readers located at ports of entry, which will be used to query the appropriate EDL data in NEDS to associate the biographical data and photo, obtained previously by the issuing authority from the traveler, and push that data from NEDS to the CBP officer.

CBP, similarly, will use the RFID number collected from the Department of State (DoS) passport card to query a copy of the DoS, federal dataset maintained in TECS. Likewise, CBP's own Trusted Traveler Program cards employ RFID chips to provide a number to the CBP RFID reader for purposes of allowing the biographical and photo enrollment data to be associated with the RFID number in GES and then pushed to the CBP officer's primary screen during the border crossing event.

The process employed to verify, electronically, the biographical data and photograph information where an issuing authority chooses to maintain the data rather than provide a copy of this data to CBP will differ from those cases where the issuing authority chooses to allow CBP to maintain a copy of the database. With these documents, such as the Washington State EDL, CBP will use RFID readers to retrieve the identifier associated with each document when it is presented at the border. CBP will then transmit this identifier through secure channels to the issuing authority's database where the identifier will be associated with the appropriate biographical data and photo. The biographical data and photograph associated with that identifier will then be retrieved from the issuing authority's database and provided to the CBP officer conducting the examination in order to process the traveler during the border crossing event and, upon completion, recording of the information and incident of border crossing in BCI and/or TECS, as appropriate. To date, a majority of non-federal information providers have chosen to follow this model.

Lastly, it should be noted that all RFID enabled border crossing travel documents and the U.S. Passport contain a Machine Readable Zone (MRZ) on the document which contains the biographical information printed on the document. In the event that the CBP RFID readers are not functioning or are not available, CBP may use the MRZ on such documents to retrieve the biographical information and compare it to the information appearing on the face of the

document, or as a final option, the data appearing on the face of the document may be manually entered by the CBP officer.

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)?

No. The information collected during border crossing operations is used to identify previously submitted biographical and biometric (photograph) data for the purpose of verifying the travel document used to denote identity and citizenship, and allow CBP to screen the traveler as part of its border security and law enforcement responsibilities. NEDS, GES, and TECS are used to perform travel document verification as part of CBP's traveler screening functionality. BCI is a repository that will enable CBP officers to view a traveler's biographic information, and if applicable, previous travel history during the system's retention period. The information recorded in BCI will be cross-referenced with data maintained in other appropriate law enforcement databases, to ensure the admissibility of travelers and to screen all passengers arriving from foreign travel points, to the United States, or departing the United States for foreign ports, 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 a law enforcement concerns.

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

For border crossings the information recorded in BCI is reviewed for accuracy at the time of the border crossing by the CBP Officer, prior to being recorded in BCI. The CBP Officer reviews the travel document provided, the information retrieved from a back-end system, and the officer's own observations and information provided by the traveler. If any information appears to be inconsistent the traveler may be referred for additional processing to clarify or resolve the inconsistency.

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 personally identifiable 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. Additionally, an officer must have a "need-to-know" for access to the information.

In the cases of shared databases, either from federal sources (*i.e.*, DoS passport cards), foreign sources (*i.e.*, Canadian provincial EDLs), or domestic non-federal entities (*i.e.*, EDLs), those datasets containing RFID enabled border crossing documents are maintained separately from the transactional functionality of TECS that is used to process border crossings. In the case of EDLs where the issuing authority chooses to provide CBP with a copy of the information, CBP will maintain the referenced dataset in a separate system of records, NEDS, if the information is provided in advance of an individual crossing the border. This information will be used to electronically validate the biographic information and photograph associated with a travel document for border crossing purposes when such a document is presented at a port of entry.

During the issuance of the travel document, an authority collects biographical and biometric information directly from the traveler. This information will subsequently be used to validate a travel document during the border crossing event by direct contact between CBP Officers and the travelers at the ports of entry. The information will be collected by running the passport or travel document through the machine readable zone (MRZ) or through the use of other technology such as radio frequency identification in documents such as a passport card so as to expedite passenger processing and ensure the accuracy of biographical information entered into CBP's systems.

In consideration of privacy, CBP has limited the sharing of NEDS data to the statutory disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act, and has not published any routine uses under 5 U.S.C. 522a(b)(3). This provides an individual possessing an approved travel document, such as EDL, whose data is shared with CBP prior to crossing the border with a similar level of privacy protection as the individual whose data is shared at the time of crossing with CBP.

For land border crossings, the information recorded in BCI will be received from various other datasets as noted above, such as DoS passports or NEDS. Those datasets automatically populates the information reviewed by a CBP officer during processing. The information will also be verified by CBP Officers checking the documents at time of arrival into the United States. Upon admission/parole into the United States, the information will be recorded in BCI.

For air and sea border crossings the information will be collected from APIS or verified with the use of e-Passport readers where deployed and applicable in addition to the information collected during in person inspection at air or sea ports of entry. The relevant information will be collected from travelers by the respective carriers/operators and submitted to CBP in advance of the traveler's arrival at the border. The submitted APIS information will be verified by a CBP Officer and recorded in the BCI following the determination to admit/parole.

In all situations, the information recorded in BCI may be cross-referenced against CBP's enforcement database systems. All relevant passport data may be verified against the Passport

Records System at Department of State. Enhanced driver's licenses may be verified against the issuing authority's database, via either means noted above. This will help to ensure accuracy of the information used by CBP during the border crossing

Section 3.0 Retention

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

The information collected from travelers as recorded within the BCI dataset 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 as recorded in BCI is used for entry screening and other law enforcement and counterterrorism purposes.

BCI data is subject to a retention requirement. The information as recorded in BCI is used for the purposes described above. For U.S. Citizens (USC) and Lawful Permanent Residents (LPR) the information is maintained for fifteen years from the date of the border crossing incident at which time it is erased from BCI. For non-immigrant aliens, the information will be maintained in BCI for seventy five (75) years from the date of the border crossing incident in order to ensure that the information related to border crossing is available for providing any applicable benefits related to immigration and for other law enforcement and counterterrorism purposes. For non-immigrant aliens who later become LPRs or United States citizens following a border crossing that leads to the creation of a record in BCI, the information related to their border crossings prior to the change in status will follow the 75 year retention period, but all border crossing information thereafter will follow the 15 year retention period applicable to USCs and LPRs. However, for all travelers, BCI records that are linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases will remain accessible for the life of the law enforcement activities to which they may be or become related.

The information collected and maintained in NEDS is used for border crossing purposes and is retained in NEDS for the duration of the validity of the travel document, that is from the date of issuance by the issuing authority until the date of expiration on the document, or, to the extent more restrictive, in accordance with the terms of any memorandum of understanding/agreement between CBP and the issuing authority. Information contained in NEDS will be retained and updated as information is provided by the issuing authority, so as to ensure timeliness, relevancy, accuracy, and completeness.

In the cases of NEDS and BCI, CBP is putting together retention schedules and will be working with NARA for approval of these schedules. Information maintained in TECS, GES, and APIS are pursuant to their published system of records notices.

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

A review of the record retention and disposition schedules for the NEDS, BCI, and TECS databases is being planned with NARA as part of the current review and updating of the TECS system of records notice and the Federal Register notice announcing the introduction of BCI and NEDS.

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

Information must be retained in BCI for a period of fifteen (15) years for USC and LPRs and seventy five (75) for non-immigrant travelers. These retention periods, generally, permit the cross-referencing and review by CBP analysts of historical data relating to individuals who cross the border and allow other components of DHS and other relevant government authorities to review and assess the appropriate issuance of immigration benefits when they may be sought and to perform a variety of enforcement functions. This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress. Organizations, which pose a threat to border security or simply intend to smuggle, employ a variety of means to establish associations and contacts on both sides of the border for the purpose of facilitating the illegal movement of people, contraband, and merchandise across the border. Often legitimate and illegitimate crossings may be paired as persons pursue their illicit activities.

Information maintained in NEDS is subject to the retention period of validity of the travel document, to allow CBP to establish the identity, citizenship and admissibility of travelers entering the United States and to enforce the laws administered by CBP at the border during the period of time when a travel document may be presented.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The information maintained in BCI 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 BCI and border crossing information within DHS is role based according to the mission of the component and need to know. Similarly, access to TECS enforcement information is role based according to the mission of the component and need to know. Among the DHS components with regular access to border crossing information are: U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (CIS), the Transportation

Security Administration (TSA), the United States Coast Guard, and the DHS Information & Analysis Directorate (I&A).

Sharing of information stored in the NEDS database will occur only where this information is necessary to verify the identity, citizenship, and admissibility of an individual when he or she attempts to enter the United States and to ensure compliance with all other U.S. laws enforced by CBP at the border, or under those circumstances where disclosures are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act. CBP has not published any routine uses of information stored in the NEDS database under 5 U.S.C. 522a(b)(3). Use of the information in NEDS will also conform with the terms of the relevant memoranda of agreement with the relevant government agency governing the relevant providing for the storage by CBP of information related to travel documents that will be accepted for border crossing purposes.

To the extent data derived from NEDS is subsequently transferred to other systems of record (e.g., upon presentment of a travel document in conjunction with a border crossing), that data may be used in a manner consistent with the system of records notice published for the receiving system of records.

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

Sharing information within DHS will be decided on a case by case basis, consistent with the mission objectives of the components involved and any relevant circumstances. In a general sense, this means that border crossing information that supports a DHS law enforcement or component mission objective may always be shared with the responsible persons charged with performing that duty. 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's 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 data from passports, EDLs, and Trusted Traveler Program cards collected and maintained in BCI as part of the border crossing event.

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. All information is kept secure, accurate and controlled.

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 personal information being misused or inappropriately used, the information, maintained in either BCI or NEDS, is shared only with DHS personnel who have established a need to know the information as part of the performance of their official duties. Internal DHS access to the BCI and NEDS 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, access to both BCI and NEDS will be limited to individuals who have successfully completed annual privacy and security training. Audit logs of access to all personal information are in place and reviewed periodically by Office of Internal Affairs.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

The information maintained in BCI may be shared on a "need to know" basis, as warranted by a particular request or an identified MOU/A with respective Federal, state, local, tribal, foreign and intergovernmental law enforcement agencies in order to support ongoing law enforcement, counterterrorism or compliance activities, with a defined scope and duration. Presently, this sharing may extend to every law enforcement or counterterrorism 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, intergovernmental law enforcement agencies and a majority of foreign nations with whom the U.S. maintains diplomatic relations.

External sharing of information stored in the NEDS database will occur only where this information is necessary to verify the identity, citizenship, and admissibility of an individual when he or she attempts to enter the United States and to ensure compliance with all other U.S. laws enforced by CBP at the border, or under those circumstances where disclosures are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, and has not published any routine uses under 5 U.S.C. 522a(b)(3). Use of the information in NEDS will also conform with the terms of memoranda of agreement with the issuing government agency governing the provision and storage by CBP of information related to travel documents that will be accepted for border crossing purposes.

To the extent data derived from NEDS is subsequently transferred to other systems of record (e.g., upon presentment of a travel document in conjunction with a border crossing), that data may be

used in a manner consistent with the system of records notice published for the receiving system of records.

5.2 What information is shared and for what purpose?

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

5.3 How is the information transmitted or disclosed?

The information in BCI, subject to sharing, may be transmitted either electronically or as printed materials to be shared with authorized personnel. CBP's external data sharing of the border crossing data is required to comply with statutory requirements, including those pertaining to national security and law enforcement. Additionally, memoranda defining roles and responsibilities, have been executed between CBP and each agency that regularly accesses TECS and, if the need to know is sufficient, BCI. Lastly, information that is shared with other agencies, Federal, state, local, tribal, or foreign governments outside of the context of any MOU requires a written request by the entity requesting the information 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, Regulations & Rulings, Office of International Trade, CBP. Requests will be evaluated for conformance with the Privacy Act, the published routine uses for TECS and BCI, and the receiving agency agrees to be restricted from further unauthorized sharing of the information. Additionally, the agency receiving the information is informed in writing of the constraints around the use and disclosure of the information at the time of the disclosure. Where permitted, the sharing of NEDS data will be in accordance with the terms of the Privacy Act, the grant of access to the issuing authorities' data and the terms of the NEDS SORN.

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 currently has Memoranda of Understanding with law enforcement agencies that have access to TECS. These memoranda address the access and use of TECS data by those agencies. With respect to BCI data, that was formerly maintained as a dataset within TECS, the access and use of this data will be subject to the same memoranda and rules for sharing.

CBP and the Canada Border Services Agency, individual states, and additional entities have or intend to enter into memoranda for the exchange of information related to travel documents that will be issued by these entities and that will be accepted by CBP for border crossing purposes.

5.5 How is the shared information secured by the recipient?

Recipients of TECS and BCI data are required by the terms of their sharing agreement (MOU/A) to employ the same or similar precautions as CBP in the safeguarding of the TECS and BCI information that is shared with them. Recipients of NEDS data will conform to the requirements of the Privacy Act, any relevant MOU/A, and to the specific terms of the authorization permitting the case by case sharing.

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

CBP requires all non-CBP users of TECS and those systems which reside upon the TECS IT platform, to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in the TECS and BCI 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 (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 limitations on use. The 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 Certificate of Authority to Operate are issued or renewed. External sharing of information maintained in NEDS will not occur through system access, and will conform with the terms of the Privacy Act, the grant of access to the issuing authorities' data and the terms of the NEDS SORN.

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 two new System of Records Notices in conjunction with this PIA, Border Crossing Information (BCI) and the Non-Federal Entity Data System (NEDS). Notice is also provided through the publication of this PIA on the internet. 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 in to or depart from the United States. Individuals may choose the type of travel document they wish to employ to cross the border, and they may choose the issuing authority to whom they provide their biographical and biometric data. This means that an individual may choose whether or not to use a travel document that will require his or her information to be maintained in NEDS (*e.g.*, an EDL issued by an authority that provides data to CBP prior to an individual crossing the border). Once an individual chooses to cross the border, she or he must present information sufficient to establish her or his identity and citizenship to the satisfaction of a CBP Officer, as determined by DHS. Upon admission/parole into the United States, this information will be recorded and maintained in BCI. To the extent associated with any enforcement action, that same information may be recorded in TECS.

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 collected in NEDS, BCI, or TECS. With respect to the use of information submitted to non-DHS and non-CBP issuing authorities, individuals should consult with those authorities regarding their right to consent to particular uses. As for the use of the information, once it is presented to CBP in a border crossing context, the individual no longer retains any rights respecting his or her consent to the use of the information.

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 or other WHTI compliant travel document and that the regulations have changed. This lack of knowledge is identified as a privacy risk because of the mandatory requirements to provide a validated travel document capable of denoting identity and citizenship. For this purpose, CBP will be providing notice through publications on its website such as "Ready, Set… Go", "Know before You Go" [www.cbp.gov/xp/cgov/travel/vacation/kbyg/], this PIA, the WHTI PIA, the RFID PIA and the several *Federal Register* publications relating to rule change concerning this regulation and the *Federal Register* notices related to the two system of records.

Section 7.0
Individual Access, Redress and Correction

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

For information maintained in BCI, no exemption shall be asserted with respect to information maintained in the system at it relates to the border crossing encounter.

This system, however, may contain records or information pertaining to the accounting of disclosures made from BCI to other law enforcement agencies (Federal, State, Local, Foreign, International or Tribal) in accordance with the published routine uses. For the accounting of these disclosures only, in accordance with 5 U.S.C. 552a (j)(2), and (k)(2), DHS will claim the original exemptions for these records or information from subsection (c)(3), (e) (8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

For information maintained in NEDS, no exemption shall be asserted with respect to information maintained in the system at it relates to the requestor's travel document.

Individuals may seek access to their information by writing or faxing an inquiry to Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511). Additionally, Individuals may seek access to their specific information by filing a Privacy Act request with the same Customer Service Center.

For information associated with a law enforcement activity or obtained and/or developed as a result of a referral for secondary screening, that information will be maintained in TECS. The

TECS system of records is exempt from the access provisions of the Privacy Act, as a law enforcement system TECS 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).)

7.2 What are the procedures for correcting erroneous information?

CBP has an Executive Communications Branch in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by BCI. If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: 877-CBP-5511). Individuals making inquiries 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.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (DHS 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 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, seaports and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous information 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 http://www.dhs.gov/trip.

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

If during an interaction with a CBP officer at the border an individual has a question, CBP had developed an information sheet that provides information about how to contact CBP's Customer Service Center. Additionally, CBP posts information on its web site for individuals to find out how to correct his/her information. If a traveler believes incorrect or inaccurate information exists about them in BCI or NEDS, the traveler, or his authorized representative, may make inquires to CBP's Customer Service Center (see section 7.2 above) or via DHS TRIP.

7.4 If no redress is provided, are alternatives are available?

Redress is provided either via DHS TRIP or by contacting CBP's Customer Satisfaction Unit directly.

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.

As part of DHS's ongoing effort to increase transparency regarding the collection of information at the Department, as well as its efforts to specifically review the personally identifiable information maintained on the TECS information technology platform, DHS and CBP have identified different data sets that call for individual notice so as to provide appropriate routine uses, retention, and exemptions to the Privacy Act. As such, DHS has chosen to minimize the number of exemptions claimed for BCI and is providing more access with that SORN. With respect to NEDS, DHS has also restricted the exemptions to those available under the Privacy Act and afford access to the submitted information. Additionally, DHS recently modified its redress and correction mechanism for individuals that need to correct data collected by a component agency of DHS, e.g., CBP. DHS TRIP is the result of the 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. The DHS TRIP may be accessed via the internet at www.dhs.gov/trip.

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 each of the systems (TECS, BCI, and NEDS) is role based and is granted and limited by consideration of a user's need to know and mission responsibility. 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. Additionally, the number and type of users with access to NEDS has been further narrowed from the universe of users with access to TECS or BCI and is limited to CBP Officers at land and sea borders in performance of official duties, and IT specialists directly assigned to support the NEDS infrastructure.

8.2 Will contractors to DHS have access to the system?

Yes, subject to the same background, training, 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. CBP personnel who have access to TECS will also have access to BCI.

Additionally information received from issuing authorities and maintained in NEDS will be maintained separately so that information from one authority is not co-mingled with information from another.

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

To gain access to the TECS, NEDS and/or BCI 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 thus BCI and NEDS). Reauthorization is dependent upon a user continuing to be assigned to a mission role requiring TECS (and BCI and NEDS) 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, NEDS, and BCI maintain audit trails or logs for the purpose of reviewing user activity. TECS, NEDS, and BCI 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, NEDS, and BCI to suspend access, automatically. Misuse of TECS, NEDS, and BCI 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 IT infrastructure (including BCI and NEDS) are required to complete and pass an annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the TECS IT infrastructure. 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 the TECS IT infrastructure. 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, BCI and NEDS datasets, as components of TECS IT Platform, are approved through TECS IT Platform Certification and Accreditation under the National Institute of Standards and Technology. The last certification was in January 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 recorded in BCI 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, now known simply as "TECS". The data module is now being

identified as Border Crossing Information (BCI) to provide more transparency into CBP's information collection and use processes. CBP previously collected border crossing and passport information and stored it within the TECS system (which includes APIS, a component of TECS).

NEDS was designed to maintain information to support the use of alternative forms of travel documents, authorized by the Secretary of DHS and issued by non-federal authorities. This information is separated by each issuing authority so that information provided by one issuing authority, such as a state department of motor vehicles, is not co-mingled with information provided by another issuing authority, such as another state department of motor vehicles.

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

The collection of border crossing information, as proposed in BCI, and the proposed storage of this information in TECS prompted the redesignation of that specific database as a separate Privacy Act System of Records: Border Crossing Information (BCI). BCI permits greater visibility to the traveling public regarding where CBP records the border crossing information of persons admitted/paroled into the United States; such visibility was not previously available when the subject information was exclusively maintained in TECS.

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

In order to maintain control over the information received from non-federal issuing authorities, the NEDS system was designed to have separate databases. Additionally, the uses of the information in the NEDS system were restricted to only those mandated to be available by the Privacy Act.

9.3 What design choices were made to enhance privacy?

The principal design choice made to enhance privacy with respect to Border Crossing Information was to create a separate and distinct System of Records under the Privacy Act to retain border crossing information for persons departing from (to the extent collected) and/or admitted/paroled into the United States. The BCI system of records, while permitting the sharing of requested information with other systems for purposes of verifying the information that had been collected from the traveler, precludes the automatic sharing of all collected information with law enforcement systems. This means that BCI will share information to confirm a match of passport or travel document data, as a means of verifying identity and confirming the instance of the border crossing, but it will not exchange information, in the form of a data dump, for the purpose of it being retained, historically, in the verifying system. BCI is the separate and distinct location for the retention of information collected upon a person's admission/parole into or, in certain instances, departure from the United States.

In developing the EDL program, DHS identified two options with regards to electronic verification of the biographic data and photograph of individuals presenting an EDL upon entering the United States at a port of entry. One option requires that a copy of the entire database holding the

biographic data and photo be shared by the issuing authority with CBP, so that CBP may access individual records as a traveler chooses to present an EDL upon crossing the border. The second option requires that CBP obtain individual biographic data and photograph from a database maintained by the issuing authority on each occasion when a traveler presents an EDL upon crossing the border. The first option requires CBP to maintain and update a database containing each governmental entity's entire border crossing travel document data set, whether or not all persons in the database are choosing to cross the border at any given time. The second option does not require CBP to maintain such a database. Both options only provide information to BCI at the time a person chooses to cross the border using an appropriate border crossing travel document. In consideration of privacy concerns, CBP created the NEDS system to maintain and use the data obtained through option one in a manner similar to its use of the information obtained through option two.

Responsible Officials

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

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

Reviewing Official:

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

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security