Privacy Impact Assessment
for the

TECS System: CBP Primary and Secondary Processing

December 22, 2010

Contact Point
Valerie Isbell
Office of Information Technology
Customs and Border Protection
(571) 468-3100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The TECS (not an acronym) System is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by the U.S. Department of Homeland Security's (DHS) component United States (U.S.) Customs and Border Protection (CBP). TECS is both an information-sharing platform, which allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of CBP and numerous other federal agencies that it supports.

TECS not only provides a platform for interaction between these systems and defined TECS users, but also serves as a data repository to support law enforcement "lookouts," border screening, and reporting for CBP's primary and secondary inspection processes, which are generally referenced as TECS Records or Subject Records. In order to provide more transparency as it relates to the functions and data in TECS, CBP published separate Privacy Impact Assessments (PIAs) and Privacy Act System of Records Notices (SORNs) for the CBP sub-systems based on the purpose and use of the information. CBP also maintains other federal agency data on TECS to stage the information for use by CBP at the time an individual presents himself/herself to CBP. This allows TECS to work more efficiently and reduces the performance impact on the originating systems.

This PIA focuses on CBP's use and modernization of TECS as it relates to the primary and secondary inspection processes (including information collected in advance of arrival, during inspections at the United States (U.S.) port of entry (POE), and retention of information and reports following interactions during U.S. border crossing activities) to ensure compliance with the numerous laws enforced by CBP, including determining the admissibility of persons attempting to enter the U.S. CBP will issue a separate PIA to address the information access and system linkages facilitated for CBP, DHS, and other federal agency systems that link to TECS and share data within the TECS user community.

Overview

Pursuant to the Homeland Security Act of 2002, the E-Government Act of 2002, and to provide expanded notice and transparency to the public, DHS/CBP is issuing this PIA for TECS as it pertains to CBP's use of TECS as a data repository in the primary and secondary screening processes to ensure compliance with the numerous laws enforced by CBP, including laws governing the admissibility of persons attempting to enter the U.S.

This PIA focuses on those aspects of TECS that relate to CBP's interaction with the general public during the various stages of international travel that involve crossing the U.S. border. Focusing on TECS and its sub-systems, this PIA discusses the collection and use of personally identifiable information (PII) from individuals during events connected to international travel into or out of the U.S., CBP primary and secondary inspection processes, and CBP enforcement actions.

DHS is charged with ensuring compliance with federal laws at the border including those preventing contraband, other illegal goods, and inadmissible persons from entering or exiting the U.S.

DHS' border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to ensure compliance with any law or regulation enforced or administered by DHS and its components, and to determine if the merchandise is subject to duty or being introduced into the U.S. contrary to law. Accordingly, all travelers entering the U.S. must undergo DHS customs and immigration inspection to ensure that they are legally eligible to enter (as a U.S. citizen or otherwise) and that their belongings are not being introduced into the U.S. contrary to law. It is not until those processes are complete that a traveler, with or without his/her belongings, is permitted to enter the U.S.

Depending on the method of conveyance used to travel to the U.S. (e.g., air, sea, land (pedestrian and vehicle)), CBP collects certain information from, and about, the traveling public at various stages of the international trip in order to perform law enforcement queries on the traveling public prior to and/or at the time of performing an inspection, including making admissibility determinations which may permit entry into the U.S. Generally, within the rubric of TECS, CBP collects information: 1) prior to arrival (e.g., Advance Passenger Information System[1]), 2) at the time of arrival (e.g., Nonimmigrant Inspection System[2], Border Crossing Information system[3]), and 3) as appropriate, throughout its inspection of the international traveling public to detail certain enforcement related circumstances (e.g., TECS[4], Seized Assets and Case Tracking System[5]). These systems are physically located within the information technology (IT) architecture of TECS with discrete SORNs in place, recognizing each system's discrete purpose, distinct authority, differing populations, access rules, and retention periods. Inclusion of these systems within the TECS IT architecture, often described as residing upon the TECS Platform, facilitates the collection and cross-referencing of these data sets as a traveler crosses the border.

For the purposes of this PIA, "Subject Records" is a generic term that will be used to describe the enforcement or inspection records located in TECS pertaining to individuals. Such records include, but are not limited to, those records related to a violation of law discovered by CBP or another authorized user agency or a CBP officer narrative concerning an interaction between CBP and a person. Subject Records encompass not only violations of laws enforced by CBP, but may also include information on violations of other federal and state laws.

Air/Sea Travel Process

In general, CBP obtains certain information about individuals traveling to the U.S. on commercial or private aircraft, as well as commercial vessels, through CBP's Advance Passenger Information System (APIS). The information obtained from APIS is screened against TECS Records and other law enforcement databases (e.g., National Criminal Information Center (NCIC)) in order for CBP to ascertain if any security or law enforcement risks exist. These pre-arrival or pre-departure TECS queries include checks against lookouts, such as "wants and warrants," watchlist matches, etc., entered by law enforcement officers or received from the Automated Targeting System (ATS)[6], previous border crossing

[1] DHS/CBP-005 Advance Passenger Information System (APIS).
[2] DHS/CBP-016 Nonimmigrant Information System (NIIS).
[3] DHS/CBP-007 Border Crossing Information (BCI).
[4] DHS/CBP-011 CBP TECS.
[5] DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS).
[6] DHS/CBP-006 Automated Targeting System (ATS).

history, including previously issued I-94 or I-94W arrival/departure records in the Nonimmigrant Inspection System (NIIS), recorded prior violations of law, and records in the Seized Asset and Case Tracking System (SEACATS).

Upon arrival in the U.S. in the air/sea environment, individuals are generally required to present themselves to CBP at the POE's primary arrival location (primary). At primary, CBP obtains information directly from the traveler via his or her presented travel documents (e.g., passport) and/or verbal communication between the CBP officer and the traveler.[7] The information collected in primary is matched against the previously provided APIS information and any Subject Records, to the extent they exist.. At this point, CBP will collect any required forms such as, the I-94 Arrival Departure Record or FinCen 105 Currency/ Monetary Instrument Report (CMIR) (a Bank Secrecy Act report concerning the international movement of more than $10,000 worth of currency). These collections, in the air/sea environment, are not an event that automatically necessitates referring a person to the secondary arrival location ("secondary").

For all individuals entering the U.S. at a POE, a record detailing the traveler's border crossing is captured through TECS and maintained in the Border Crossing Information System (BCI).

If the CBP officer at primary determines that additional inspection is needed, the traveler will be referred to secondary. A record of the referral and secondary inspection is entered into TECS as a Subject Record. During a secondary inspection, a CBP officer may run law enforcement queries through TECS and other systems on the TECS Platform. Regardless of the outcome of the secondary inspection, the CBP officer will create a record of the secondary inspection in TECS. If the secondary inspection results in a violation being discovered, then a record may also be created in SEACATS.

If the CBP officer at primary determines that there are no admissibility issues, and any other issues that might have arisen are successfully resolved, then an individual will be permitted to proceed to collect their baggage. At some ports of entry, admissibility processing, customs clearance (also referred to as baggage control), and inspections for compliance with the statutes and laws governing the importation of agriculture occur simultaneously. While obtaining their baggage, travelers may also interact with a CBP officer or CBP agriculture specialist who may question arriving travelers, particularly about issues related to their baggage or agricultural items. This interaction may entail simple questioning or a more thorough inspection of the traveler and their possessions, including baggage.

Land Travel Process

Unlike the air/sea travel where CBP has received APIS, CBP generally does not receive information about individuals traveling to the U.S. by foot (pedestrian) or vehicle prior to their arrival at the POE. There are no manifests required for travelers or private passenger vehicles entering the U.S. by land. In certain instances, CBP may receive voluntary submission of passenger manifests for rail and commercial bus traffic across the U.S. border. Additionally, with regard to commercial vehicle traffic,

[7] At certain airport locations individuals who have been successfully enrolled in a CBP trusted traveler program may be processed through CBP primary by scanning their designated trusted traveler document at an approved kiosk, or by otherwise complying with the requirements of their specific trusted traveler program. The Global Enrollment System (GES) PIA discusses the PII that is submitted to CBP as part of a trusted traveler application.

CBP receives the cargo manifest, which also contains information concerning the driver and any passengers, one hour prior to arrival.[8]

Primary and secondary inspection processes will vary based on the different POE because of geographical and logistical realities. In some POEs primary and secondary will occur at the same time with the same CBP officer., While in other POEs primary and secondary will be in different locations with more than one CBP officer.

Pedestrian Process

Pedestrians are required to present themselves to CBP at a designated POE upon arrival in the U.S. At primary, the CBP officer at primary obtains information directly from the pedestrian via the travel documents presented by the traveler (e.g., passport, other border crossing credential, and verbal communication) and verifies the information. The CBP officer at primary will conduct a TECS query to see if there are prior CBP violations that might indicate a need for further review as well as queries against lookouts, such as "wants and warrants," terrorist watchlist, etc.

If the CBP officer at primary determines that there may be an issue requiring further inspection, such as concerns regarding admissibility, agriculture, or customs (baggage), then the traveler, typically, will be referred to another CBP officer at secondary for processing. At the time of the referral to secondary, the CBP officer at primary creates a record in TECS. Pedestrians who are required to obtain an I-94 or I-94W will be referred to secondary for processing, but this action does not mean that the CBP officer at primary will create a separate Subject Record of the inspection in TECS. For all individuals entering the U.S. at a POE, a record detailing the traveler's border crossing is captured through TECS and maintained in the BCI.

A CBP officer at secondary may perform simple questioning or a full inspection relating to issues such as admissibility, customs (baggage), or agricultural issues, based on the circumstances. During an inspection at secondary, the CBP Officer may run law enforcement queries through TECS and other systems on the TECS Platform. If the secondary inspection results in a violation being discovered, then a record may also be created in SEACATS.

Vehicle Process

Vehicles are presented to CBP at the vehicle primary border crossing lanes upon arrival at a land POE. At vehicle primary, the CBP officer obtains information directly from the driver and traveler(s) within the vehicle via their travel documents (e.g., passport), and/or verbal communication. Vehicle border crossing lanes may also contain license plate readers, which assist in querying the license plate numbers of vehicles approaching primary. Additionally, vehicle border crossing lanes may contain radio frequency identification (RFID) readers, which will query applicable travel documents that are within the vehicle.[9]

[8] http://www.dhs.gov/files/publications/gc_1281020492905.shtm, under "ACS/ACE".
[9] http://www.dhs.gov/files/publications/gc_1281020492905.shtm, under WHTI.

The information collected at vehicle primary is used to query TECS to assist the CBP officer in determining the admissibility of the person(s) and otherwise inform the CBP officer charged with enforcing other U.S. laws at the border. The CBP officer at primary will conduct a TECS query to see if there are prior CBP violations that might indicate a need for further review as well as queries against lookouts, such as "wants and warrants," watchlist matches, etc. Additionally, the CBP officer at primary will conduct searches based on the license plate information.

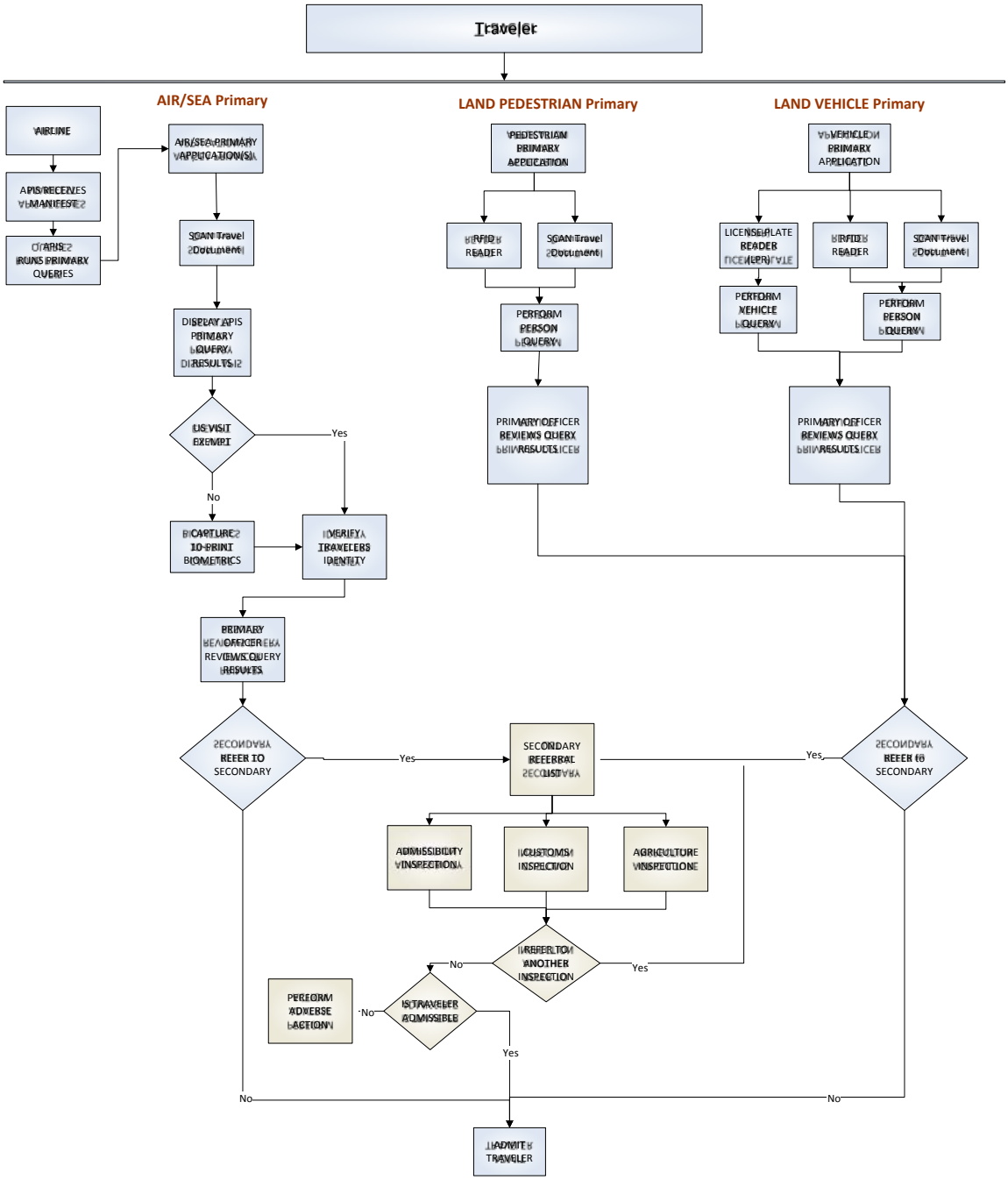
If the CBP officer at primary determines that further examination is appropriate (for example, to address concerns related to admissibility, customs, and agriculture laws), then the vehicle and all of its occupants will be referred to vehicle secondary for processing. Where an individual within a vehicle is required to obtain an I-94 or I-94W prior to admission, the vehicle and all its occupants will be referred to secondary for processing, but this action does not mean that the CBP officer at primary will create a separate Subject Record of the inspection in TECS. During a vehicle secondary inspection, a CBP officer may run law enforcement queries through other systems on the TECS Platform. A record of the secondary is entered into TECS. If the secondary inspection results in a violation being discovered, then a record may also be made in SEACATS.

TECS Modernization

TECS Modernization is a multi-year update to the basic operation and functionality of TECS. The improvements include enhancements to the graphical user interface and, as well programming changes to integrate and automate the exchange of information and officer referrals from primary inspection to secondary inspection. Presently, the TECS user interface is a static text and menu-driven screen manipulated by users through function keys and manually entered commands. The new user interface being developed will employ graphical icons, permit the use of pointing devices (e.g., a mouse), allow for the incorporation of photos and other biometric images, and provide for the use of interactive screen icons to input data and perform functions.

The planned enhancements to information management and workflow incorporated into TECS Modernization focus on providing CBP officers with a single screen for initiating and recording reports of activities and queries of persons and their information performed during primary and secondary inspection. At its most basic level, TECS Modernization will allow an officer at secondary to access, view, and input information on the screens and records viewed and used by the officer encountering the traveler at primary. This capability to share the operational view of a traveler's progress through the entirety of CBP's inspection and admissibility processes not only improves efficiency, but also reduces the incidence of false positives by permitting the CBP officer at secondary to cross reference and verify the referral action made by the CBP officer at primary. The goal of TECS Modernization is to simplify the functional operation of TECS for the CBP officer/user so as to permit the CBP officer to direct more of his or her efforts toward interacting with the traveler or person crossing the border. These technical changes do not impact the purposes and uses of the information maintained on the TECS platform such as APIS, BCI, and SEACATS.

Figure 1: Primary to Secondary Flow



This PIA covers TECS as the primary repository for enforcement related activities at the border. A separate PIA will be forthcoming that will separately address the technology for the TECS Platform and provide a more detailed discussion on the interaction TECS has with other law enforcement systems. (See the Appendix for a list of systems with which TECS interacts.)

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

As part of processing individuals at the border, DHS/CBP conducts pre-arrival or pre-departure TECS queries, which include checks against lookouts, such as "wants and warrants," watchlist matches, etc., entered by law enforcement officers or received from the ATS and confirmed by a CBP officer based on threshold targeting rules. The fact that an individual may need additional inspection will be noted in TECS as a Subject Record.

During CBP's primary and secondary inspection processes, CBP may collect the following information in TECS:

- Complete name (last name, first name, and middle name or initial);
- Social Security number;
- Date of birth;
- Address;
- Telephone number;
- Citizenship;
- Gender (F=Female; M=Male);
- Photo image (where available);
- Occupation;
- Driver's license information;
- Import/export information;
- Currency and other CMIR information;
- Pleasure boat and private aircraft information;
- Travel document information, including passports, visas, permanent registration cards, driver's licenses, etc. Information includes: document number, country of issuance, city of issuance, consulate of issuance for visas, document type (P=Passport; V=Visa; A=Alien Registration), issuance date, and expiration date;
- Country of residence;
- Alien registration number (where applicable);
- U.S. address while in the U.S. (number and street, city, state, zip code);
- International Air Transport Association (IATA) arrival port code;
- IATA departure port code;
- Seaport of departure and/or arrival;

- Flight/tail/voyage number (as applicable);
- Date of flight/voyage arrival;
- Date of flight/voyage departure;
- Airline/vessel carrier code;
- U.S. border crossing event history (where applicable);
- License plate numbers (as read and forwarded by the license plate reader system or manually entered by the CBP Officer) for all vehicles entering and leaving the U.S.; and
- Fingerprint Identification Number (FIN) (where available).

Additionally, free-form text may be entered into certain record types by TECS authorized users. The free-form text that is entered is intended to contain comments about certain events that are not collected electronically by TECS, but have been determined necessary to properly reflect the context of a record or an activity.

Information retained by other systems for which there is a TECS interface, which is requested to be displayed by a TECS user, is displayed with the content unaltered. An example would be data returned by NCIC as a result of a query originating in TECS. Upon verification that the NCIC result is a positive match to the TECS query, a Subject Record is created.

1.2 What are the sources of the information in the system?

Data located in TECS is collected both directly and indirectly from the public. Information is obtained directly from travelers during CBP primary or secondary inspections or as a result of a CBP enforcement action, such as a seizure of merchandise. The information is also obtained directly from a traveler's travel documents and indirectly through cross-referencing with other systems such as APIS and BCI or via direct access to another system. Information in TECS may also be collected from individuals while departing the U.S.

Subject Records that are acquired from other agencies through linked access to their law enforcement systems are expected to comply with the rules of those systems concerning sources and methods of acquisition of information.

Other federal, state, local, and international law enforcement entities may also provide lookouts and other law enforcement information that will be stored in TECS regarding a person of interest. TECS maintains a copy of the FBI's Terrorist Screening Database (TSDB). This information may be entered directly by those agencies that are authorized TECS users or may be entered on behalf of those agencies by CBP.

TECS provides CBP specifically authorized users with access to Nlets, formerly known as the National Law Enforcement Telecommunications System, which is owned by states of the U.S. and provides standard driver license and vehicle queries to criminal history and Interpol information, as well as California Law Enforcement Telecommunications System (CLETS), which provides similar information for the State of California. Nlets links together and supports every federal, state, local law

enforcement, justice, and public safety agency for the purposes of sharing and exchanging critical information.

1.3 Why is the information being collected, used, disseminated, or maintained?

Relevant data, including PII, is necessary for CBP to effectively and efficiently perform its inspection, including assessing the admissibility of a person attempting to enter the U.S. This assessment includes analyzing the potential risk and/or threat posed by a person or a conveyance that is entering or exiting the U.S. Data entered, retained, and communicated by TECS is intended for use by authorized users of the system in order to facilitate CBP counterterrorism, law enforcement, border security, and inspection activities, and the numerous other federal agencies that it supports.

CBP enforces many different agencies' laws at the border (e.g., U.S. Department of Agriculture (USDA)) requirements on Plant and Pest Quarantine, and the Drug Enforcement Administration (DEA)'s restrictions on the importation of controlled substances), as such, other agencies have access to TECS and are able enter information related to individuals who have or may have violated the law and for which CBP is able to take action upon that individual when CBP encounters that individual. For example, TECS maintains a copy of the FBI's Terrorist Screening Database (TSDB). CBP uses that information to determine whether or not individuals should be able to enter the country.

1.4 How is the information collected?

Certain information in TECS is collected directly from the traveler or his/her travel documents during interaction with CBP. If any enforcement activity is undertaken with respect to an individual at a CBP POE, a record of such action is recorded in TECS. Separately, the CBP Officer possesses the discretion to enter a record in TECS for any interaction with a member of the public. If a violation of law is discovered (e.g., undeclared merchandise at a POE) information related to the violation is entered into TECS. In these situations, information will be taken directly from the subject individual, to the greatest degree possible, consistent with the nature of the violation. Furthermore, information relating to violations or lookouts may be entered into TECS by representatives from TECS user agencies consistent with those agencies' law enforcement or compliance mission.

1.5 How will the information be checked for accuracy?

Collected data is routinely compared to existing records to ensure that accurate information is maintained. Information that is collected directly from the traveler or person will be checked for accuracy through direct comparison of the person to the travel document and/or other forms of identification. CBP relies on other systems to have appropriate processes in place to ensure the accuracy of the data being shared through TECS.

Because of the law enforcement and border security context in which TECS is used, it is sometimes impractical and inconsistent with the manner in which law enforcement information may be obtained to directly verify the accuracy of information with the individual about whom the specific

information pertains. However, because TECS is used by multiple agencies both within DHS and outside, users other than the data owner who hold relevant knowledge may provide the data owner with corrections for inaccuracies when they are discovered. Users that have access may directly query source databases or other government databases to verify the accuracy of TECS information; when source systems are updated, TECS will also be updated based on the manner in which TECS receives information from the source system (electronically or manually entered).

Additionally, CBP has instituted an Officer-initiated function in TECS to address certain issues pertaining to some records that may contain conflicting information. This function is referred to as the Primary Lookout Override (PLOR) function. The PLOR function was developed to assist travelers who are erroneously designated for secondary inspections because they possess a characteristic similar to a person of interest. PLOR allows CBP Officers to override certain TECS Records where a similar biographical trait exists between the traveler and another person who is the subject of a TECS Record, provided that the non-subject traveler is able to provide a unique characteristic that differentiates him or her from the person of interest. The PLOR procedures require supervisory approval before a PLOR record may become active. All such amended transactions are logged by TECS and attributed to the authorized user performing the correction. This includes any required supervisory approval.

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

The collection of manifest information from all passengers and crew members, which is screened through TECS, was mandated by Congress in the Aviation and Transportation Security Act of 2001 (ATSA), Public Law 107-71, 115 Stat. 597; the Enhanced Border Security and Visa Reform Act of 2002 (EBSA), Public Law 107-173, 116 Stat. 543; 49 U.S.C. § 44909 (applicable to carriers operating passenger flights in foreign air transportation to the U.S.); 8 U.S.C. § 1221 (applicable to commercial flights and vessels arriving in and departing from the U.S.); and CBP general statutory authority including 19 U.S.C. §§ 1431 and 1644a (requiring manifests for vessels and aircraft). Additionally, CBP has general authority to conduct searches and detentions at the border, for example: 8 U.S.C. §§ 1225 and 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, and 1595a(d); 22 U.S.C. § 401; and 31 U.S.C. § 5317, as well as the attending regulations of CBP promulgated at Titles 8 and 19 of the Code of Federal Regulations. For a more comprehensive list of applicable authorities relevant to data collected in TECS, please refer to the individual PIAs for the TECS systems/sub-systems in the Appendix.

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

TECS is established as an overarching law enforcement information collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database. This environment is comprised of several modules designed to collect, maintain, and screen data as well as conduct analysis, screening, and information sharing. The system is accessed for data entry, communication, and query by approximately 70,000 authorized users, including personnel

from government agencies outside of CBP and DHS. There is a risk that too much information is being maintained and used in TECS. In light of the volume of records maintained and the number of authorized users of TECS, all users must undergo a background investigation (BI) prior to granting access. In addition to this threshold criterion for access, CBP also employs several layers of training, review, and access control. All users are required to read and comply with the TECS security requirements, as well as take and pass the TECS Security and Privacy Awareness course annually in order to establish and retain TECS access. Supervisory review is required to ensure that only authorized records are entered and the information is accurate. CBP's Office of Internal Affairs has functions that allow it to monitor the use of TECS. Extensive audit logs are maintained showing who has accessed records and what changes, if any, were made to the records. Lastly, access to TECS is controlled by both the physical location and mission responsibilities of the user (e.g., a CBP officer at primary at a port on the Southern border will not have immediate access to information collected at a port along the Northern border).

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

CBP uses TECS to document the interactions with individuals at the border when there is a possible violation of a law that is enforced by CBP either through its own specific authorities or those vested in it by another agency. TECS information is used to support the law enforcement and counterterrorism mission of CBP, DHS, and other federal, state, local, international, and foreign law enforcement agencies with law enforcement, intelligence, and counterterrorism responsibilities. TECS query capabilities can be used to analyze data from various sources to assist authorized users in the identification of areas of law enforcement interest, concern, or relationships indicating the possible presence of such interests/concerns.

In addition to the above uses, CBP's ATS employs Subject Records as part of its screening of individuals. ATS will cross-reference Subject Records as part of its process of running an individual's information against the threshold targeting rules. Matches to a Subject Record or a threshold targeting rule require further review by a CBP officer and may also result in additional inspection. The fact that an individual has a Subject Record does not necessarily mean that individual will always match a threshold targeting rule.

The Appendix of this PIA indicates the systems/sub-systems and functions that are incorporated within TECS and those separate from TECS, which are queried by TECS, to support the primary and secondary inspection processes.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Authorized users may employ TECS query capabilities to analyze data from various sources to assist in the identification and comparison of similar and dissimilar aspects of previously unknown areas of law enforcement interest and concern.

TECS Modernization, a planned enhancement to the functionality of TECS relating to primary and secondary processing, will include deployment of High Performance Primary Query (HPPQ) and Consolidated Secondary Inspection Service (CSIS). HPPQ provides an updated replacement for the backend processing of law enforcement queries conducted in primary by providing CBP officers at primary with faster TECS query capabilities. HPPQ allows the primary CBP officer to more effectively conduct law enforcement checks while simultaneously facilitating legitimate travel.

CSIS provides CBP officers with an updated graphic user interface (GUI) for processing travelers referred to secondary. CSIS allows the CBP officer in secondary the ability to authenticate a referred individual's identity displaying the same photograph that was available during primary processing. The databases associated with the travel documents presented during primary (e.g., visa, passport) are the source for the photos displayed in CSIS. The sources for the photo databases include the U.S. Department of State's databases for passport and visa photos, U.S. VISIT photographs collected by CBP, and U.S. Citizenship and Immigration Service (USCIS) Lawful Permanent Resident (LPR) photos. Additionally, when enhanced driver's licenses (EDL) are used as the travel document, photographs from EDL participating agencies may be reviewed. Copies of these photograph databases may be maintained on the TECS platform in order to meet "real time" capability requirements.[10] In addition to photographs, CSIS displays the reason for the referral to the CBP officer in secondary.

TECS Subject Records are one of the data sources for ATS, which also uses threshold targeting rules to identify individuals and cargo that may merit additional inspection.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

TECS does not receive direct feeds of information from commercial data aggregators, and it does not collect direct feeds from public news sources. Officers may incorporate publicly available information into narrative reports contained in TECS if the CBP officer determines that the information is relevant to the analysis being performed. Such incorporation is at the discretion of the CBP officer and is not the result of an automated collection.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There is a privacy risk that information may be misused by CBP officers. Access to Subject Records is controlled at the record level as well as at the system level through administrative passwords and restrictive rules regarding access to the CBP Intranet, as well as the TECS database. Examples of the types of access controls include: system entry validation; individual accountability; auditing; resource access control; and security administrator control. In addition, the authorized users are limited to the roles defined for their use of the system. Furthermore, all authorized users of TECS have had a BI, taken and

[10] Copies of Enhanced Driver's License (EDL) photo databases are accessed at the time an individual seeks to cross the border. See DHS/CBP-008 Non-Federal Entity Data Systems (NEDS).

passed the annual TECS Security and Privacy Awareness course, and are given information on a "need-to-know" basis only. Procedural and physical safeguards are utilized, such as accountability, receipt records, and system audits.

System access to information in TECS by authorities outside of DHS is also governed by both a Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA) [note: ISAs are required to establish networking, hardware, and security protocols for non-DHS systems to connect to DHS systems]. Furthermore, CBP relies and adheres to the "Third Agency Rule" with respect to the dissemination of Subject Records that are owned by another agency. Simply, this means that information accessed and viewed through TECS cannot be disclosed outside of TECS and others who use TECS by the accessing agency without specific approval of the agency or entity which owns (i.e., first collected and submitted) the data being accessed.

Section 3.0 Retention

3.1 What information is retained?

TECS retains Subject Records, inspection reports, and information obtained from TECS sub-systems or accessed systems, which supports the narrative contained in the Subject Record or inspection report. This retention is consistent with the published Privacy Act SORN for TECS (December 19, 2008, 73 FR 77778). Some of the information that is retained in TECS may include information retained in TECS sub-systems (e.g., BCI). Information that is contained in a TECS sub-system is retained for a period consistent with that sub-system's SORN. In addition, TECS retains audit logs pertaining to all user's keystrokes and access sessions, for purposes of ensuring compliance with the safeguarding and security protocols pertaining to TECS.

3.2 How long is information retained?

Subject Records and inspection reports are retained by TECS for a maximum of 75 years from the date of last collection of data, with updates occurring on a transactional, as-needed basis. A Subject Record is only created by the TECS user (e.g., CBP Officer, ICE Special Agent), if there is an enforcement interest in the subject or the subject is connected to an enforcement action. The Subject Record may be updated to add, modify, or delete certain content in the record. Subject Records may be deleted by an authorized user, or the person responsible for placing the record in TECS, if the user's supervisor authorizes that action. In all cases, TECS logs the action taken by each authorized user on data records.

Additionally, systems and sub-systems of TECS, (e.g., APIS, BCI, and NIIS) have their own retention periods. For a description of those systems and sub-systems and their respective retention periods, please see their published Privacy Act SORNs listed on the DHS Privacy Office website at www,dhs.gov/privacy.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Subject Records retention schedules have been reviewed by CBP's records officer. CBP is in the process of obtaining approval from NARA for the current retention schedule that conforms to the Privacy Act SORN published in December 2008.

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

CBP has determined it needs to maintain the Subject Record for a period of 75 years to support determinations of admissibility in accordance with the Immigration and Naturalization Act. Persons may travel to the U.S. throughout their lifetime and access to relevant past interactions between a person and the government assist CBP Officers in assessing the potential risk posed by the person, and whether or not the person may be admitted to the U.S. Of the data retained by TECS, the Subject Record produced after an enforcement incident is of concern when evaluating the privacy considerations of creating and retaining such a record. This is due to the fact that CBP creates and updates the Subject Record as a result of enforcement interest in or encounter with the subject in question, in accordance with CBP policy and procedures; the record directly pertains to the person/subject, and is used to inform future encounters with the subject. The record is updated when the nature or status of the enforcement interest changes or CBP becomes aware that the information contained within the record requires an update. In all cases, CBP enforcement personnel will apply applicable policy, procedure, and law in dealing with the subject. The retention of the Subject Record is deemed necessary to equip CBP enforcement personnel with all facts known about the subject that are consistent with CBP enforcement interests in the subject.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared, what information is shared and for what purpose?

Consistent with DHS regulations and the One DHS policy, the information collected in TECS may be shared with all DHS components that show a need to know the information, consistent with the component's mission. The following DHS components or offices currently receive or have access to TECS information:

- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Secret Service (USSS)
- U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)

- DHS Inspector General (IG)
- Transportation Security Administration (TSA)
- Office of Intelligence and Analysis (I&A)

The objectives of sharing TECS data within the DHS community are: 1) to provide the DHS enforcement community a common repository with query capability that houses information gleaned from and about suspected or known violators of the law; 2) to provide the ability for timely communication of information related to known or suspected criminals to the CBP Officer or other DHS employee, such as ICE Agents; and 3) to provide a common repository for the routine recording of law enforcement activity, including investigations, inspection results, and assets that may be seized from criminals as a result of law enforcement activities.

4.2 How is the information transmitted or disclosed?

TECS information may be transmitted either electronically or as printed materials to authorized personnel.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In order to mitigate the privacy risks of PII being misused or inappropriately used, DHS personnel must establish a need to know the information as part of their official employment duties to access the information. Additionally, internal DHS access to the data is controlled by CBP through the use of strict access controls for the users, passwords, background investigations on individuals who have access to the data, as well as system audits that track and report on access to the data. Furthermore, all TECS users are required to take and pass the annual TECS Security and Privacy Awareness course in order to establish and retain TECS access. Supervisory review is required for creating records, such as Subject Records, to ensure that only authorized records are entered and the information is accurate. CBP's Office of Internal Affairs has functions that allow it to monitor the use of TECS. Extensive audit logs are maintained showing who has accessed records and what changes, if any, were made to the records.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared, what information is shared and for what purpose?

TECS information may be shared with agencies that have demonstrated a justifiable need for the TECS information. Authorization for an outside entity's access to TECS is granted by the TECS Program Manager (in concurrence with all necessary DHS/CBP offices) and authorized via a MOU between DHS/CBP and the outside entity. An Information Sharing Agreement will also be utilized to cover any interface implemented between DHS/CBP and an outside entity. The MOU specifies the general terms

and conditions that govern the use of the functionality or data, including privacy-related limitations on use, and the types of information in TECS to which the agency is being granted access, depending upon its mission needs. The ISA specifies the data elements, format and interface type to include the operational considerations of the interface.

TECS information may also be shared with outside federal, state, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies in the absence of a MOU. Typically, the requesting or receiving agency must be able to identify or have identified a need-to-know, a specific purpose for the information, and a use that is consistent with a routine use published in the most recent TECS Privacy Act SORN.

The TECS information that is shared with agencies outside of CBP is the same information that is shared internally. This information usually entails existing TECS Records pertaining to an enforcement action, illegal activity or suspected illegal activity associated with the subject party. The TECS information is shared with external agencies for law enforcement, counterterrorism, and border and public security purposes.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, sharing of TECS information outside the Department is compatible with the border security and law enforcement purposes for which the information in TECS is collected. For example, the Privacy Act SORN for TECS has several routine uses which provide for sharing in a law enforcement context with federal, state, local, tribal, foreign, and international law enforcement agencies. In addition, the Privacy Act SORN for TECS contains routine uses to permit sharing with agencies in the intelligence community, when the need to know has a nexus to border security.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Access to Subject Records is also governed by a need-to-know criteria that demands that the receiving entity demonstrate a mission related need for the data before access is granted. The reason for the access, the scope of its use, and the purpose to which it will be employed are the primary privacy related concerns that are included in both the initial and ongoing authorization (MOU and ISA) that is negotiated between CBP and a respective agency seeking access to TECS.

TECS information may be transmitted or disclosed to external agencies through approved methods. All TECS users are required to read and comply with the TECS security requirements, as well as take and pass the annual TECS Security and Privacy Awareness course in order to establish and retain

TECS access. Currently, CBP has several MOUs with external agencies covering the sharing of Subject Records.

Alternatively, if the agency seeking the TECS information does not have an electronic interface into TECS, appropriate TECS Records will be transmitted pursuant to the terms of the MOU between CBP and the agency or on a case-by-case basis.

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

When sharing TECS information with parties outside of DHS, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to Subject Records is governed by a "need to know" criteria that demands the receiving entity demonstrate the mission related need for the data before access is granted. The reason for the access, a specific mission purpose, and an intended use consistent with the receiving agency's purpose and CBP's justification for collecting the data, are also concerns that are included in either the terms of a negotiated MOU and ISA or the language of an authorization providing facilitated access to an external agency. 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, including the operational considerations of the interface. MOUs and ISAs are periodically reviewed, and outside entities must agree to use, security, and privacy standards before Certificates to Operate (CTO) are issued or renewed.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes. Individuals attempting to enter into the U.S. are required to provide information in the form of a DHS approved travel document as well as any necessary forms (e.g., I-94 form, FinCEN 105). CBP has posted signs at POEs providing notification of the information or forms required. This signage, CBP's website, the Privacy Act SORN for TECS, and the associated PIA for TECS provide individuals with notice of what CBP's requirements are for entering into the country. Additionally, during a secondary inspection CBP will provide individuals further notice regarding any additional information required.

CBP uses the information collected to query TECS Records to ascertain whether or not the individual is previously known to the law enforcement community. If that query produces no results, the individual's information is processed by the CBP Officer as part of the inspection process and for purposes of admissibility into the U.S. The information will be stored in the BCI System, or other appropriate system, such as the NIIS, and may be shared in accordance with the routine uses for those Privacy Act SORNs.

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

Generally, there is no opportunity for an individual to decline to provide information that is required in order to travel to enter the U.S. Pursuant to CBP's border search and immigration authority, an individual seeking entry into the U.S. must satisfy the CBP Officer that he/she is a U.S. citizen, LPR or otherwise eligible for admission to the U.S., and that he/she is not attempting to import or export any merchandise in violation of U.S. laws.

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. The information maintained in TECS is required to be submitted prior to admission to the U.S. and is used to determine eligibility to enter the U.S.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection of information are mitigated.

There is a risk that the individual may not know that their information is being maintained in TECS in the ways described. Accordingly, CBP has published the Privacy Act SORN for TECS and this PIA to increase the transparency of its operations.

Section 7.0 Access, Redress and Correction

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

The Secretary of Homeland Security has exempted TECS from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, CBP will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in TECS, or seeking to contest its content may gain access to certain information in TECS about themselves by filing a Freedom of Information Act (FOIA) request with CBP at:

U.S. Customs and Border Protection

FOIA Division

799 9th Street NW, Mint Annex

Washington, DC 20229-1177

7.2 What are the procedures for correcting inaccurate or erroneous information?

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

U.S. Customs and Border Protection

CBP Info Center

Office of Public Affairs

1300 Pennsylvania Avenue

Washington, DC 20229

Travelers may also contact DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

Additionally, CBP has instituted an Officer-initiated function in TECS to address certain issues pertaining to some records that may contain conflicting information. This function is referred to as the Primary Lookout Override (PLOR) function. The PLOR function was developed to assist travelers who are erroneously designated for secondary inspections because they possess a characteristic similar to a person of interest. PLOR allows CBP Officers to override certain TECS Records where a similar biographical trait exists between the traveler and another person who is the subject of a TECS Record, provided that the non-subject traveler is able to provide a unique characteristic that differentiates him or her from the person of interest. The PLOR procedures require supervisory approval before a PLOR record may become active. All such amended transactions are logged by TECS and attributed to the authorized user performing the correction. This includes any required supervisory approval.

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

No individual notification of procedures for correcting TECS Records is currently provided. TECS contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notification to individuals that they are or have been the subject of a law enforcement investigation would undermine the performance of the law enforcement mission of CBP. However, inasmuch as mistakes in TECS may exist, requests for redress should be directed the avenues listed in Section 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal redress is provided through the avenues mentioned in Section 7.2.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

TECS is a law enforcement application that retains sensitive data on individuals that are primarily subject to an enforcement action or are suspected of or known to be violators of the law. Consequently, the fact that CBP has created and retained records on an individual often stems from the fact that the individual is suspected of or known to be in violation of the law. Accordingly, Privacy Act access and procedural rights have been limited. However, CBP recognizes that TECS also maintains records related to certain activities that are not necessarily illegal (e.g., border crossing activities). In light of this, CBP has segregated those systems and sub-systems and published separate Privacy Act SORNs to address this unique aspect of TECS.

In general, the data collected and retained by TECS that identifies an individual is typically provided by the individual as the result of processing at the U.S. border, and in some circumstances may be certified by that individual as accurate as part of that process. Data reflecting inspection results, suspected commission of crimes, associations with known criminals, and other enforcement related comments is typically entered by DHS enforcement personnel and appended to the data that was originally provided by the individual. However, CBP regularly reviews its processes for redress and is currently modifying the redress and correction mechanism for individuals that need to correct collected data. Part of this effort is reflected in Section 7.2.

Section 8.0 Technical Access and Security

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

In order to gain and maintain access to TECS information, a user must have, at a minimum, the appropriate BI and successfully take and pass the annual TECS Security and Privacy Awareness course, well as have a need to know TECS information. An agency representative (CBP supervisor or agency National System Control Officer (SCO)) submits the request to CBP indicating the individual has a need to know for official purposes. CBP verifies that the necessary BI and security and privacy training have been completed prior to issuing a new user account.

Every new and existing user of TECS is assigned an SCO. The SCO is responsible for the user's profile record and assigns the role(s) and the functions within that role. The SCO may assign only functions for which the SCO has authority to use, as well as authority to assign. User accounts are reviewed periodically and certified annually to ensure that these standards are maintained.

8.2 Will Department contractors have access to the system?

Yes. CBP employs contract personnel for TECS analysis, programming, testing, and operations support. These contract personnel undergo the same BI and security and privacy training as CBP

personnel. Their access to TECS is granted to facilitate their delivery of tasks, as defined by their respective contract. Other DHS contractors may have similar access.

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

Initial TECS access is not activated for an individual without completion of the TECS Security and Privacy Awareness course and a successful score on the associated test. The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides a number of sharing and access scenarios to test the prospective user's understanding of appropriate controls put in place to protect privacy. A user must pass the course test scenarios to gain and retain access to TECS. This training is regularly updated and TECS users are required to take the course annually.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The TECS application has been Certified and Accredited (C&A) in accordance with the requirements defined under the Federal Information Security Management Act (FISMA). The most recent C&A for TECS was completed in December 2008. Additionally, the TECS Modernization effort, a multi-year upgrade to the TECS system and functionality, received its initial C&A in July 2009.

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

TECS maintains audit trails or logs for the purpose of reviewing user activity. TECS actively prevents access to information for which a user lacks authorization, as defined by the user's role in the system, location of duty station, and/or job position. Multiple attempts to access information without proper authorization will cause TECS to suspend access automatically. Misuse of TECS Records can subject a user to criminal and civil penalties, as well as discipline in accordance with the CBP Code of Conduct, which can include being removed from one's position. The TECS Platform PIA discusses the auditing procedures in greater detail.

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

Privacy risks identified with respect to access and security were the inappropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, the CBP Code of Conduct and Disciplinary system, and criminal and civil penalties. Additionally, CBP employs a practice of least privileged system access, which limits the ability of a user to access information that exceeds the mission scope of the user's assigned duties.

Section 9.0 Technology

9.1 What type of project is the program or system?

TECS is a "legacy" application that was developed in-house in the late 1980s by the former U.S. Customs Service.

TECS is currently undergoing a system-wide technological upgrade, referred to as TECS Modernization, which is changing the presentation, format, and overall operating environment supporting TECS.

9.2 What stage of development is the system in and what project development lifecycle was used?

TECS is an operational system.

The initial phase of TECS Modernization is currently deployed at five CBP POEs, and is awaiting approval for deployment to additional sites in a fully operational capacity.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss its implementation.

TECS was designed as a centrally-deployed system run on a mainframe environment. Best practices for system and application security were incorporated as part of the overall design, including but not limited to, integrating TECS Privacy and Security Awareness course completion into access authorization to TECS and supervisory approval requirements for a majority of the information entered into TECS. Currently, TECS runs on a mainframe located within CBP. TECS Modernization will provide all of the functionality provided by legacy TECS, however operations will move to a distributed system. TECS Records are available via secure web interfaces to a limited number of agencies and field support personnel via the CBP Vetting subsystem. TECS Modernization, including CBP Vetting, utilizes FIPS 140-2 compliant federally mandated encryption standards to protect privacy data.

Responsible Officials

Valerie Isbell, Executive Director, Passenger Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection, (571) 468-3100.

Kim Mills, Director, Traveler Entry Programs, Office of Field Operations, U.S. Customs and Border Protection, (202) 344-1438.

Laurence Castelli, CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, (202) 325-0280.

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

As mentioned above, TECS is both a repository of different data sets and an information sharing platform. Below you will find three tables:

- Table 1 describes the data that resides on the TECS Platform and is collected by CBP and covered by a CBP Privacy Act SORN.
- Table 2 describes data that resides on the TECS Platform but was not collected by CBP and is covered by another Federal Agencies' Privacy Act SORN. The information resides on TECS in order to allow TECS to meet its operational needs to respond quickly so as not to have lines at the border.
- Table 3 describes the systems that are accessible through TECS but for which the data does not actually reside.

TECS has the following sub-system and linked system interfaces that may be utilized as described above and in the relevant Privacy Act SORNs and PIAs. Please note that several of the systems/sub-systems referenced below may have separate Privacy Act SORNs and/or PIAs published. For a more detailed discussion of the systems/sub-systems please see the appropriate document listing on the DHS Privacy Office website at www.dhs.gov/privacy.

Table 1 Sub-systems – Data that resides on the TECS Platform and is collected by CBP

Sub-system	***Privacy Act – System of Records Notice – Federal Register***	***Published or Pending PIA***	***General Comments***
Advance Passenger Information System (APIS)	73 Fed. Reg. 68435	YES	See APIS PIA and SORN for more information on APIS. These documents can be found on the DHS Privacy Office website at www.dhs.gov/privacy.
Border Crossing Information (BCI)	73 Fed. Reg. 43457	YES	See BCI PIA and SORN.
Global Enrollment System (GES)	71 Fed. Reg. 20708	YES	See GES PIA. Principal system for collecting and storing information on individuals who have enrolled in a CBP trusted traveler program.
Non-immigrant Information System (NIIS) - I-94 and I-94W data/query	73 Fed. Reg. 77739	NO	See NIIS SORN.
Seized Asset and Case Tracking System (SEACATS)	73 Fed. Reg. 77764	PIA currently Pending for Publication	See SEACATS SORN.

Table 2 Data that resides on TECS but is not collected by CBP

Sub-system or Interface Name	***Privacy Act – System of Records Notice – Federal Register***	***Published or Pending PIA***	***General Comments***
Interface with U.S. Department of State: Passport Information Electronic Records System (PIERS)	73 Fed. Reg 16602008	YES	PIERS is a U.S. Department of State system.
Interface with Non-Federal Entity Data System (NEDS)	73 Fed. Reg. 43462	Yes	States with Enhanced Drivers Licenses
Interface with U.S. Citizenship and Information Services: Alien File (A-File) and Central Index System (CIS)	72 Fed. Reg. 1755	Yes	USCIS provides data from the Central Index System (CIS) on persons entitled to lawful permanent residence, refugees, and asylees, all classes of persons whose information is maintained by DHS as being entitled to special procedures regarding admissibility under the Immigration and Naturalization Act.
Interface with the DHS Watchlist Service	73 Fed. Reg. 77778	Yes	In accordance with the Watchlist Service PIA (July 14, 2010), Watchlist information for CBP is maintained in TECS

Table 3 Data that is accessible through TECS but does not reside on TECS

Sub-system or Interface Name	***Privacy Act – System of Records Notice – Federal Register***	***Published or Pending PIA***	***General Comments***
National Crime Information Center (NCIC)	64 Fed. Reg. 52343	YES	NCIC is U.S. Department of Justice system.
NLETS (formerly known as the National Law Enforcement Telecommunications System)	NO	NO	Owned by the states of the U.S., not subject to PA or E-Gov.
California Law Enforcement Telecommunications System (CLETS)	NO	NO	See above.
Canadian Police Information Center (CPIC)	NO	NO	Foreign agencies are not subject to PA or E-Gov.