Privacy Impact Assessment
for the

TECS System: Platform

DHS/CBP/PIA-021

August 12, 2016

Contact Point
John Maulella
Office of Field Operations
Customs and Border Protection
(202) 344-2605

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security, U.S. Customs and Border Protection owns and operates the TECS (not an acronym) system. The TECS Platform facilitates information sharing among federal, state, local, and tribal government agencies, as well as with international governments and commercial organizations. CBP's mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies. Through the TECS Platform, users are able to input, access, or maintain law enforcement, inspection, intelligence-gathering, and operational records. CBP is publishing this Privacy Impact Assessment as a complement to the previously published DHS/CBP/PIA-009, CBP Primary and Secondary Processing PIA from 2010, to provide notice to the public and to assess the privacy risks and mitigations associated with the TECS Platform.

Overview

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 United States.[1] 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 United States contrary to law. DHS/CBP's mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies.

Accordingly, all travelers entering the United States 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 United States 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 United States.

Depending on the method of conveyance used to travel to the United States (*e.g.*, air, sea, or land (pedestrian and vehicle)), CBP collects certain information from, and about, the traveling public at various stages of the international trip. As part of the inspection and admissibility process, CBP performs law enforcement queries on the traveling public prior to and/or at the time of performing an inspection, including making admissibility determinations that may permit entry into the United States. Generally, CBP collects information:

[1] *See* authorities listed in Section 1.0.

1) Prior to arrival in the United States (*e.g.*, Advance Passenger Information System[2]),

2) At the time of arrival (*e.g.*, Nonimmigrant Inspection System,[3] Border Crossing Information system[4]), and

3) As appropriate, throughout its inspection of the international traveling public to detail certain enforcement related circumstances (*e.g.*, TECS,[5] Seized Assets and Case Tracking System (SEACATS)[6]).

These different types of information collections are physically located within the information technology (IT) architecture of TECS with discrete System of Records Notices (SORN) in place, recognizing each system's discrete purpose, distinct authority, differing populations, access rules, and retention periods. The 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.

TECS System

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 CBP. TECS is both an information-sharing platform, "TECS 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 law enforcement system, "TECS,[7]" that includes 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 different types of information (*e.g.* APIS, BCI, TECS, and SEACATS) 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. 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 the TECS module of the TECS Platform 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.

---

[2] DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015, 80 FR 13407.
[3] DHS/CBP-016 Nonimmigrant Information System, March 13, 2015, 80 FR 13398.
[4] DHS/CBP-007 Border Crossing Information (BCI), January 25, 2016, 81 FR 404.
[5] DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.
[6] DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.
[7] DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

TECS Compliance Framework

In order to provide more transparency as it relates to the functions and data in TECS, CBP published separate Privacy Impact Assessments (PIA) and Privacy Act System of Records Notices (SORN) 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.

TECS privacy compliance documentation is divided into three categories:

1. TECS Primary and Secondary Inspections Process – CBP conducted a PIA in 2010 to describe 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 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 United States. The information collected pertaining to an individual's travel forms the operational basis for much of the TECS system and is discussed in more detail in the CBP Primary and Secondary Processing PIA,[8] as well as in section 1.2 of this PIA.
2. TECS Platform – This PIA describes TECS Platform, which includes 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. The TECS Platform, which houses many of these records and provides a portal to several other systems and services to facilitate screening, vetting, and analysis activities for CBP and external agency users.
3. TECS source systems – Covered by their own individual PIAs and SORNs, as noted in the Appendices to this PIA.

TECS Platform

The TECS Platform is the underlying infrastructure designed to facilitate the maintenance and sharing of law enforcement, inspection, intelligence-gathering, and operational records among the TECS user community. TECS is also used by other agencies, known as Partner Government Agencies (PGA), which are provided with access to TECS (for a full list of current PGAs with access to TECS, please see Appendix 4). The TECS Platform serves as a mechanism to query the databases of other law enforcement agencies, and serves as a centralized platform to

[8] DHS/CBP/PIA-009, CBP Primary and Secondary Processing, and DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* http://www.dhs.gov/privacy

access CBP and other PGA records. TECS maintains records that are owned by CBP, and records that are owned by external agencies. External partner agencies that input records into TECS, without a Lookout record, are maintained by the external partner agency for purposes of the Privacy Act of 1974.[9] Records maintained within TECS that are owned and maintained by CBP include information about individuals who have violated, or are suspected of violating, a law or regulation that is enforced or administered by CBP (to include Lookout records uploaded by other agencies); to provide a record of inspections conducted at the border; to determine admissibility into the United States; and to record information regarding individuals, vehicles, cargo, firms, and organizations to whom the Department of Homeland Security (DHS)/CBP has issued detentions and warnings. TECS also retains records on individuals who have been given access to the system for authorized purposes. TECS information is maintained in multiple databases that have been integrated into a single information technology architecture – known as the "TECS Platform" – in order to facilitate timely collection and comprehensive cross-referencing of datasets.

This Privacy Impact Assessments (PIA) reviews the framework in which TECS Platform data is maintained, describes the data security and auditing mechanisms by which this data is secured, and evaluates the methods by which data is shared or restricted among DHS/CBP and the other international, national, federal, state, local, and tribal agencies and commercial organizations. CBP has previously published separate PIAs to address the use of TECS as it relates to the primary and secondary inspection processes[10] at ports of entry, as well as procedures for processing travel documents at the border.[11]

TECS Platform Access

The TECS Platform functions as a data repository through which users are able to access different databases and perform functions and services according to their defined permissions. Users access information via their online access profile, which is defined according to each individual TECS user's particular job roles and responsibilities, known as a "TECS Profile"; the management of TECS profiles is discussed in detail in section 8.3. Accordingly, a "TECS user" is someone from CBP (or other DHS component) or another law enforcement entity at the federal or state level who has access to TECS. CBP and (when appropriate) the PGA assess access according to the user's responsibilities to enable the TECS user to access only information within the scope of his or her professional responsibilities. TECS users must generally be U.S. nationals. However, there is a limited exception for Foreign Service nationals who support missions overseas, including those who support CBP attachés, U.S. Immigration and Customs

[9] 5 U.S.C. § 552a.
[10] DHS/CBP/PIA-009, CBP Primary and Secondary Processing, and DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* http://www.dhs.gov/privacy
[11] DHS/CBP/PIA-004(e), Western Hemisphere Travel Initiative (WHTI) and DHS/CBP/PIA-007, Electronic System of Travel Authorization (ESTA), *available at* http://www.dhs.gov/privacy

Enforcement (ICE) foreign offices, or the U.S. Department of State (DOS). ICE provides access to TECS data for local and tribal law enforcement agencies.[12]

The TECS Platform contains datasets that, while being physically located within the TECS IT architecture, are covered by different SORNs and PIAs, as mentioned above. A list of the applicable PIAs and SORNs for each of these TECS subsystems, as well as an outline of their functions is provided in Appendix 1.

The TECS Platform is also a mechanism for querying the databases of other law enforcement agencies, and for hosting Lookout records input by other agencies for CBP to take action at Primary or Secondary Inspection (see previously published 2010 PIA[13] for more information on this process). For example, authorized users can use the TECS Platform to query records maintained within the Federal Bureau of Investigation (FBI) Criminal Justice Information Service's (CJIS) National Crime Information Center (NCIC); Interstate Identification Index (III); the International Justice & Public Safety Network (Nlets); and the Nlets interface to Canadian Police Information Centre (CPIC).[14] A full list of the systems external to CBP that TECS users may query is available in Appendix 2.

1. Types of TECS Access Levels

With more than 90,000 users, TECS requires a sophisticated and configurable access control process. CBP grants access to TECS based on four different access levels:

- Access Level 1: Data that is available to all TECS users with an appropriate type of background investigation.
- Access Level 2: Data that is available only to employees of the agency that entered the data. This level is no longer in use.
- Access Level 3: Data that is available to classes of users based on the owning agency, specifying that the information be made available to a set of users.
- Access Level 4: Data that is restricted to specific individuals as specified, or the individual creating the record (reserved for Grand Jury data).

For basic, Level 1 access, CBP requires that all TECS users must have a completed and favorably adjudicated background investigation of one of the types listed below. Background investigations must be periodically updated. The frequency at which reinvestigation is required

[12] *See* DHS/ICE/PIA-004(a) - ICE Pattern Analysis and Information Collection (ICEPIC) Update (October 26, 2011), *available at* http://www.dhs.gov/privacy.
[13] DHS/CBP/PIA-009, CBP Primary and Secondary Processing, and DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* http://www.dhs.gov/privacy
[14] Information on the NCIC is available at https://www.fbi.gov/about-us/cjis/ncic. Information on Nlets is available at http://www.nlets.org. The Privacy Impact Assessment for the Canadian Police Information Centre is available at http://www.rcmp-grc.gc.ca/en/privacy-impact-assessment-canadian-police-information-centre.

depends on the level of the initial investigation. Access to TECS functions and data will be limited depending on the type of background investigation that has been completed. The initial background investigation for all TECS users must be one of the following:

- Type 1: Access National Agency Check with Inquiries (ANACI), as defined by Office of Personnel Management (OPM).[15] Users with this type of background investigation may have access to any of the functions authorized for the user's agency, and access to data from TECS agencies when specifically granted this access by the owning agency.
- Type 2: Background Investigation (BI), as defined by OPM. Users with this type of background investigation may be given access to any of the functions and data authorized for use by the agency.

External TECS user agencies are responsible for ensuring that none of their personnel will serve as a TECS user without one of these types of completed background investigations. Full TECS access requires a BI. All external TECS user agencies must conduct an annual review of their TECS users to ensure that each user has a properly completed and active background investigation.

2. User Functionality

All TECS users have the option of designating the data they enter into TECS as access Level 1, 3, or 4, and specifying which TECS users may access this data. All TECS users, as part of training and on-boarding agreements, understand and agree that any data designated as Level 1 will be accessible to **all** TECS users. Level 1 may be disseminated to other TECS agencies, without prior notification to CBP.

All external TECS users must sign a Memoranda of Agreement (MOA) with CBP that outlines their access levels and roles and responsibilities as a TECS user. A typical TECS agreement includes the following provisions:

a) Data Access: External TECS users are typically granted access to the following types of records:

1. TECS Level 1 records.
2. TECS Level 3 and 4 records owned by the external TECS agency itself, and entered into TECS at the option of the external agency.
3. TECS Level 3 and 4 records owned by another TECS User Agency, with that other owning agency's authorization. This authorization will be documented

[15] Per Office of Personnel Management and DHS/CBP Security Policy, reinvestigation is required every ten (10) years for the ANACI and every five (5) years for the BI.

by a memorandum from the owning agency to the CBP TECS Custodian of Records, explicitly stating the class of records and access to be granted.

4. Primary Query History (PQH) records. These are records of the primary queries made at ports of entry that can be used to identify individuals or vehicles entering the country, and may include queries in support of Border Patrol activities at checkpoints.
5. Images associated with accessible records.
6. Inspection Results Records: These records are the results of CBP secondary inspections at ports of entry. They provide the disposition (*e.g.*, admitted at B2 or adverse action) and short comments on the inspection.
7. I-94 Records: These records include the entry and exit information from I-94, I-94W, and I-95 forms for most travelers other than U.S. citizens or lawful permanent residents.

b) Access to Functions: TECS users are typically granted access to the following sets of functions:

1. User Profile Record (UPR) Functions: These functions allow TECS users to create, modify, retrieve, and display records describing users of the system.
2. Subject Record Creation and Update: These functions allow TECS users to create, modify, and/or delete records on person, business, vehicle, vessel, and aircraft subjects. All records created by external agencies that are *not* considered Lookout records, are owned and maintained by the creating external agency. DHS/CBP does not assert ownership, accuracy, or Privacy Act coverage to these non-DHS and non-Lookout records.
3. Subject Query Functions: These functions allow TECS users to retrieve and display records on person, business, vehicle, vessel, and aircraft subjects based on query parameters. These functions also allow access to primary query history (crossing information), inspection results, and I-94 data.
4. Record Linking: This function retrieves and displays records that are related to records found during a subject query.
5. Management Information (MI) Reports: These functions allow TECS users to request formatted reports for display or printing.
6. Printing: This function allows TECS users to print records or groups of records retrieved through query functions or reports obtained through the MI function.

7. Primary Query History: This function provides on-line query and display, or off-line reports, of historical information on primary queries performed at ports of entry.
8. Batch Access for vetting purposes. External users are provided with access to the TECS CBP-vetting web capability that allows for the submission of data files to TECS for screening of persons of interest to the external agency. The response data from this query will also be provided in a batch file format.
9. System Support: This function includes help, an on-line user guide, access to edit tables, and a variety of other general functions.
10. Reference Library (RL) Function: This function includes an on-line user guide for available TECS systems.

TECS is the repository for data from many separate agency sources. This data includes sensitive law enforcement information. Each agency supplying data is considered to be the owner of that data and is responsible for its content and validity.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

While the authority for each specific database is described in the appropriate SORNs and PIAs listed in Appendix 1, the data collected in TECS is generally authorized by CBP's general statutory authority, including the following statutes and regulations:

- Homeland Security Act of 2002;[16]
- Tariff Act of 1930, as amended;[17]
- Aviation and Transportation Security Act of 2001;[18]
- Enhanced Border Security and Visa Reform Act of 2002;[19]
- Section 103(a)(1) of the Immigration and Nationality Act (INA) of 1952, as amended;[20]

[16] Pub. L. 107-296, 116 Stat. 2135.
[17] 19 U.S.C. §§ 66, 1433, 1459, 1485, 1624, 2071.
[18] Pub. L. 107-71, 115 Stat. 597.
[19] Pub. L. 107-173, 116 Stat. 543.
[20] 8 U.S.C. § 1103(a)(1), to enforce and administer the immigration laws (as defined in section 101(a)(17) of the INA) with respect to matters within the jurisdiction of CBP.

- Title 8 of the United States Code, Aliens and Nationality;[21]
- 18 U.S.C. Chapter 27 (customs crimes);[22]
- Title 19 of the United States Code, Customs Duties;[23]
- Illegal Exportation of War Materials;[24]
- Search and Forfeiture of Monetary Instruments;[25]
- Passenger Manifests;[26] and
- CBP regulations promulgated pursuant to Titles 8, Aliens and Nationality, and 19, Customs Duties, of the Code of Federal Regulations.[27]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Data from the following CBP systems of records is maintained in the TECS Platform IT architecture:

- *DHS/CBP-005 Advance Passenger Information System (APIS)*: This SORN 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, that is (or may subsequently be) mandated or provided on a voluntary basis.
- *DHS/CBP-007 Border Crossing Information (BCI)*: This system collects and reviews border crossing information regarding persons entering and (if applicable) exiting the United States.
- *DHS/CBP-008 Non-Federal Entity Data Systems (NEDS):* This system supports the use and collection of certain travel documents, such as Enhanced Driver's Licenses, issued by other government authorities, such as states, Canadian provinces, or Canadian territories.

[21] 8 U.S.C. §§ 1185, Travel control of citizens and aliens; 1221, Lists of aliens and citizen passengers arriving and departing; 1225, Inspection by immigration officers; and 1357, Powers of immigration officers and employees.
[22] Available at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-27
[23] 19 U.S.C. §§ 482, Search of vehicles and persons; 507, Officers to make character known; assistance for officers; 1431, Manifests; 1461, Inspection of merchandise and baggage; Examination of baggage; 1499, Examination of merchandise; 1581, Boarding vessels; 1582, Search of persons and baggage; regulations; 1595a, Forfeitures and other penalties; and 1644a, Ports of Entry.
[24] 22 U.S.C. § 401.
[25] 31 U.S.C. § 5317.
[26] 49 U.S.C. § 44909.
[27] Available at https://www.gpo.gov/fdsys/pkg/CFR-2012-title8-vol1/pdf/CFR-2012-title8-vol1.pdf and https://www.law.cornell.edu/cfr/text/19/chapter-I

- *DHS/CBP-009 Electronic System for Travel Authorization (ESTA)*: This web-based application and screening system is used to determine whether certain aliens are eligible to travel to the United States under the Visa Waiver Program.
- *DHS/CBP-011 U.S. Customs and Border Protection TECS*: This system of records consists of the enforcement, inspection, and intelligence records relevant to the anti-terrorism and law enforcement mission of CBP and other federal agencies that use TECS. The purpose of this system is to track individuals who have violated or are suspected of violating a law or regulation that is enforced or administered by CBP, to provide a record of any inspections conducted at the border by CBP, to determine admissibility into the United States, and to record information regarding individuals, firms, and organizations to whom DHS/CBP has issued detentions and warnings.
- *DHS/CBP-013 Seized Assets and Case Tracking System*: This system collects and maintains seizure data and information about current, former, and suspected violators of customs, immigration, agriculture, or other laws and regulations enforced and administered by DHS/CBP.
- *DHS/CBP-016 Nonimmigrant Information System (NIIS)*: This system maintains arrival and departure information collected from foreign nationals entering and departing the United States. on such forms as the I-94, I-94W, or through interviews with CBP officers.

The information contained in TECS Platform datasets or sub-systems is detailed in separate PIAs and SORNs. A comprehensive list of the systems that reside on, interface with, and are accessed through the TECS Platform are listed in Appendices 2, 3, and 4.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. A system security plan has been completed for the TECS application as part of the Certification and Accreditation (C&A) process 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 2014. Additionally, the TECS Modernization effort, a multi-year upgrade to the TECS system and functionality, received its initial C&A in December 2009, with a new Authority to Operate (ATO) issued in December 2014. Both TECS and TECS Modernization are included in the current Security Authorization Package.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The TECS Platform retains each subset of data according to the specific retention schedule described in each subset's SORN. As of the date of publication of this PIA, CBP is in the process of obtaining approval from NARA for the current retention schedules that conform to the associated SORNs.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Most of the information maintained within the TECS Platform is covered by the Paperwork Reduction Act, if it is not law enforcement-related. Information collections approved by OMB are described in the subsystem SORNs and PIAs. Specific information collections relevant to passenger information collections include:

1. OMB 1651-0088 – Passenger and Crew Manifest for Passenger Flights
2. OMB 1651-0103 – Passenger List/Crew List
3. OMB 1651-0107 – Application for Waiver of Passport or Visa
4. OMB 1651-0111 – Arrival and Departure Record

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The TECS Platform collects, uses, and disseminates information from CBP and PGA systems as outlined in the Appendices to this PIA. The TECS Platform is comprised of several modules designed to collect and maintain Lookout, Screening, Travel Document, Encounter, User Profile, and Audit data from the source databases and subsystems, as described in the Overview and covered in the PIAs and SORNs listed in Appendix 1. Generally, CBP collects information on individuals prior to arrival (*e.g.*., APIS), at the time of crossing (*e.g.*., NIIS, BCI), and throughout the inspection process of the international traveling public to document enforcement encounters, actions, and observations (*e.g.*., when a traveler is referred to Secondary Inspection (TECS: if law enforcement action is taken, SEACATS: if a seizure occurs)). The collection of this information is described in detail in the TECS Primary and Secondary

Processing PIA.[28] PGAs provide data, either for ingestion into TECS or through a query of the source system, when the information is relevant to CBP's missions. For example, Department of State passport information is ingested into TECS so that a CBP Officer can quickly verify a person's identity and passport information.

Lookout Records Services

TECS Lookout Records Services provide access to create, maintain, or query Lookout record information. A TECS Lookout record may be created by CBP, or other TECS partner agencies. Lookout records are created based on law enforcement, anti-terrorism, travel document fraud, or other interests (for example, if a traveler to a medical outbreak area posed a public health threat). Such interests are based on previous violations of law, suspicion of violations, or a business or occupation in which the law enforcement community has an interest. Lookout records created by external agencies are considered under the control of CBP, with a nexus to border security, because they are used by CBP Officers at primary and secondary inspection processing at the ports of entry.

TECS Lookout Records Services provides authorized users with the ability to create a Lookout Record and indicate whether the system should notify the record owner if the record is queried by another user or displayed as part of an encounter. The notification provides the record owner with the date, time, and location of query or encounter. A Lookout Record is limited to providing only enough identifying information to correspond to a particular individual or conveyance when queried, as well as an explanation of the reason for the Lookout. Authorized users may further place the Lookout Record "on Primary," which informs CBP officers at Ports of Entry of what action (if any) is required to be taken when the subject of a Lookout Record is encountered crossing the border. For example, the Lookout may indicate that a subject is armed and dangerous, requires visa verification, or should be referred to secondary inspection for further customs, immigration, or agriculture inspection by CBP Officers.

Screening Services

TECS Screening Services supports a number of system interfaces that enable authorized users to query TECS Lookout Records, NCIC and Nlets, and encounter data (including crossing, arrival, departure, secondary inspection, and air manifest information); users access this information in support of screening, intelligence, and vetting activities. CBP's collection of this information is discussed in detail in the TECS System: CBP Primary and Secondary Processing PIA.[29] In conjunction with Lookout Records Screening, the TECS Platform maintains external interfaces with the DHS Watchlist Service (WLS), NCIC/Nlets, and customized vetting services.

[28] DHS/CBP-013, Seized Assets and Case Tracking System, *available at* http://www.dhs.gov/privacy
[29] DHS/CBP/PIA-009, CBP Primary and Secondary Processing, and DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* http://www.dhs.gov/privacy

Examples of vetting services include queries of border crossing history, Non-Immigrant Information System (NIIS) information, etc. DHS WLS data is provided by the Terrorist Screening Center (TSC) and shared with DHS and its components on a need-to-know basis, as documented in the DHS/ALL/-027(b) DHS Watchlist Service PIA Update.[30] Additionally, NCIC/Nlets service provides a real-time interface to the FBI CJIS, NCIC, NCIC III, Nlets, and Nlets interface to CPIC.

Travel Document Services

CBP holds a repository of travel document records and associated border crossing histories as part of the TECS Platform. Travel document records stored within the repository are non-CBP travel-related records such as Department of State passports (including ePassports), immigrant visas (IV), and non-immigrant visas (NIV); and U.S. Citizenship and Immigration Services (USCIS) Lawful Permanent Resident (LPR) cards and other travel documents. Additionally, the Travel Document Services provides access to Enhanced Tribal Cards (ETC) and Enhanced Drivers Licenses (EDL) that are queried by CBP at primary, but are not shared with other agencies through the TECS Platform. This information is collected through system-to-system interfaces, which are listed in Appendices 2 and 3. The specific data elements of these travel documents are enumerated in the relevant Department of State, USCIS, and CBP SORNs.[31]

Encounter Data Services

Encounter data services provide access to information collected during a traveler's encounter with CBP while entering or exiting the United States. The TECS Primary and Secondary Processing PIA[32] references "subject records" to describe information collection as part of a traveler or vehicle encounter with CBP at either a port of entry or checkpoint. Encounter Data includes Currency and Monetary Instruments Report (CMIR) data, border crossing history, NIIS data, Memorandum of Information Received (MOIR) reports[33] and Secondary Inspection reports.[34]

---

[30] DHS/ALL/PIA-027(b), DHS Watchlist (WLS) Update, *available at* http://www.dhs.gov/privacy

[31] *See* Overseas Citizens Services Records-STATE-05 (May 02, 2008), Passport Records – STATE-26 (March 24, 2015), and Visa Records – STATE-39 (October 25, 2012), *available at* https://foia.state.gov/Learn/SORN.aspx. *See* CBP/DHS-005, Advance Passenger Information System (APIS), DHS/CBP-016, Non-immigrant Information System (NIIS), DHS/ICE-001, Student and Exchange Visitor Information System (SEVIS), DHS/USVISIT-001 Arrival and Departure Information System (ADIS), DHS/USCIS/ICE/CBP-001, Alien File, Index, and National File Tracking System, *all available at* http://www.dhs.gov/privacy

[32] DHS/CBP/PIA-009, CBP Primary and Secondary Processing, and DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* http://www.dhs.gov/privacy

[33] CBP officers and agents may use a free-form text field in TECS to document observations or interactions with an individual at the border; these reports are known as Memoranda of Information Received (MOIRs).

[34] DHS/CBP-007, Border Crossing Information (BCI) System of Records Notice, *available at* http://www.dhs.gov/privacy

TECS Security Services

TECS Security Services consists of three components: Internal Affairs and Background Investigation Support; User Access Management; and Auditing. These components provide built-in checks to ensure data residing on the Platform is accessed by only those who have a need-to-know (a job function requiring access to the information) and designated authority to receive the data accessed. The components also monitor TECS to ensure that users are not inappropriately accessing or using their data.

User Profile and Maintenance Data

The TECS Platform maintains information specifically about TECS users and the actions users take in the system. CBP collects information about the user as part of the application process to obtain TECS access, including complete name (last name, first name, and middle name or initial), Foreign Service National indicator, Social Security number,[35] badge number, work and home addresses, telephone numbers, occupation, supervisor's names, background investigation status, security clearance level, and certifications (i.e., NCIC and TECS Privacy Awareness certified). CBP maintains historical background investigation data on the TECS Platform to verify user access. However, the current system of records for background investigation information is the Integrated Security Management System (ISMS).[36] TECS access rights are verified through ISMS to determine whether CBP employees and contractors have the appropriate background investigation required for access to the TECS system. CBP shares user profile data on the TECS Platform on a limited basis with auditors, internal affairs personnel, and other individuals who have a need-to-know to perform their job functions.

Audit Data

Audit logging captures the activity of a user accessing TECS including user identifier, date, time, and location of the access, as well as the type of activity performed. The system captures all query requests and results, including search attempts for which the user is denied access to the results. Logs are also maintained related to the creation of TECS records, including TECS Lookout Records.

2.2 What are the sources of the information and how is the information collected for the project?

The TECS Platform is a repository of data collected directly by CBP, datasets collected by other DHS components, and data sourced from other federal, state, and international government agency systems of records that resides on, or is accessed through, the TECS

[35] CBP is transitioning away from the SSN-generated HashID for CBP users on modernized TECS. CBP is looking into an alternate Federal ID for non-CBP users but for the time being, SSN is still used for authentication.
[36] DHS/ALL/PIA-038 Integrated Security Management System, *available at* http://www.dhs.gov/privacy

Platform. *See* Appendices 2 and 3 for a list of TECS interfaces. TECS also maintains limited information on individuals who have been granted access to the system, as explained above.

DHS-collected Data

Traveler information in TECS is collected directly and indirectly from travelers while entering and exiting the United States. Data collected directly from travelers includes border crossing information obtained during CBP primary inspections,[37] documentation of a physical inspection of a traveler or their baggage in an "incident log" as a part of secondary inspection or as a result of a CBP enforcement action, such as a seizure of merchandise. Some of this information consists of notes on information collected from electronic devices pursuant to a border search.[38] CBP obtains travel document information in advance of a traveler's arrival or departure through APIS from air, land, and sea carriers. CBP also obtains travel document information through Trusted Traveler programs.[39] Separately, as explained above in the Encounter Data section, CBP Officers may record an interaction with a member of the public when it is anticipated that information pertaining to that encounter may be of future value. This is typically done in situations when a violation of the law is discovered in order to provide context, and/or to establish or supplement a Lookout record. The CBP Office of Professional Responsibility also uses the TECS Platform to track background information garnered from background investigations. Since the development of DHS's ISMS, the TECS Internal Affairs background investigation feature is used by internal affairs for historical purposes and by Office of Information Technology (OIT) to verify whether a user has the appropriate background investigation required for systems access. TECS interfaces with other DHS systems, such as the U.S. Citizenship and Immigration Services (USCIS) Person Centric Query Service and Central Index System.[40]

TECS user information is collected directly from the user. Historical information in TECS related to users' background investigations were collected through CBP Office of Professional Responsibility; the background information was gathered both directly from the subject, as well as persons interviewed in the course of the background investigation. Training and audit records are collected as part of an automated process on the TECS Platform.

Other Government Agency Data

The TECS Platform is not only a repository of enforcement, inspection, operational, and

[37] As described in the BCI SORN, CBP maintains information for each instance of an individual's entry into the United States at official ports of entry including airports, land border crossings, or sea ports. Border crossing information includes biographic and biometric information, photographs, information provided by commercial carriers, and the time of the location of the border crossing.
[38] DHS/CBP/PIA-008, Border Searches of Electronic Devices, *available at* http://www.dhs.gov/privacy.
[39] DHS/CBP-002, Global Enrollment System, *available at* http://www.dhs.gov/privacy.
[40] DHS/USCIS/PIA-010, Person Centric Query Service and DHS/USCIS/PIA-009, Central Index System, *available at* http://www.dhs.gov/privacy.

security records, but also an information-sharing platform through which the TECS user community facilitates the processing of international travelers and checks for possible links to terrorism or law enforcement violations. CBP enforces many different agencies' laws at the border. Thus, CBP affords other agencies access to TECS to view and enter data on the TECS Platform consistent with each respective law enforcement agency's legal authority to do so, and in conformance with memoranda of understanding/agreement executed between CBP (or the legacy U.S. Customs Service) and the PGA. Accordingly, the TECS Platform includes data from other federal, state, local, tribal, and foreign law enforcement entities. This data is provided to TECS via system-to-system interfaces and/or through online user input. Information collected by CBP and other DHS components can be shared by, and supplemented with, other local, state, national, foreign, and international law enforcement entities' systems via system-to-system interfaces. TECS also allows direct access to other major law enforcement systems, so that authorized TECS users may query CJIS, NCIC, Nlets, and CPIC, and others in order to obtain law enforcement information regarding persons of interest, including Lookouts.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The TECS Platform receives advance passenger information from commercial carriers pursuant to its statutory mandate.[41] TECS does not receive direct feeds of information from commercial data aggregators, and it does not collect direct feeds from public news sources. TECS users may incorporate publicly available information into narrative reports contained in TECS (such as MOIRs) if the user determines that the information is relevant to the analysis or action being performed. Such incorporation is the result of an action taken by a TECS user and is not the result of an automated collection.

2.4 Discuss how accuracy of the data is ensured.

TECS users routinely compare newly collected data to existing records to ensure that the information is accurate. For example, CBP Officers verify information received through APIS or entered into a Lookout by comparing it to identification cards and answers to questions provided by an individual at the border. CBP relies on the originating systems to have appropriate processes in place to ensure the accuracy of the data being shared through TECS. When discrepancies are discovered, CBP works with the source system owner to determine the accurate version of the information and resolve any discrepancies.

[41] The Aviation and Transportation Security Act of 2001, Pub. L. 107-71, 115 Stat. 597, and the Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. 107-173, 116 Stat. 543, provide specific authority for the mandatory collection of certain information on all passenger and crewmembers that arrive in, transit through, or depart from the United States via private aircraft, commercial air, or vessel carrier (and in the case of air carrier crew, overfly the United States).

2.5 Privacy Impact Analysis: Related to Characterization of the Information

In addition to the risks and mitigation described in previous TECS PIAs, the following potential risks related to TECS Platform's collection of data have been identified:

Privacy Risk: TECS aggregates data from many systems, including those belonging to federal, state, local, tribal, and foreign law enforcement agencies, which may exceed the minimal amount of data necessary to satisfy CBP mission responsibilities.

Mitigation: CBP maintains a large the amount of information in TECS from a variety of agencies, and while this information is necessary to CBP's mission at the border, this risk is mitigated through the employ of access controls to ensure that users can only access information relevant to their specific role. Different types of information from these agencies are required to enforce the wide spectrum of laws enforced at the border. For example, federal and state criminal violations may affect the admissibility of an alien or alert a CBP Officer to smuggling or other customs violations. Passport, visa, ETC, and EDL information assists CBP Officers in confirming the identity of the person seeking admission to the United States. Notes in narrative reports from previous inspections or MOIRs help CBP identify past violations or, conversely, rule out otherwise suspicious behavior. Moreover, access to the information in TECS is controlled by both the mission responsibilities and the role of each TECS user. Information provided to, or accessible by, PGAs is limited to those data sets that fall within their authorized missions and are delineated in a TECS MOU/MOA.

Additionally, CBP is mitigating this risk by identifying datasets that should no longer be maintained on the TECS Platform through TECS Modernization. Certain datasets currently maintained on the TECS Platform as a result of legacy operations under the U.S. Customs Service (including some ICE case management records; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) records; and Internal Revenue Service (IRS) investigative records that are inaccessible to CBP), are being migrated out of the TECS Platform to the owning agencies. CBP is migrating these records off of the TECS Platform to ensure CBP only maintains the minimal amount of information necessary to achieve its missions.

Privacy Risk: Because TECS contains a substantial amount and variety of Personally Identifiable Information (PII) collected by multiple organizations and maintained across multiple systems, there is a risk that users have access to more PII than is required to perform their specific function.

Mitigation: This risk is partially mitigated through CBP's securing of the data and the provision of user access according to a set of permissions based on need-to-know and job function. CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. CBP protects the data through uninterrupted monitoring in conformance to

National Institute of Standards and Technology (NIST) standards, to include encryption, electronic firewalls, and physical location within secured facilities. CBP restricts access to these areas to authorized users who have appropriate clearances and permissions, in the performance of their official duties.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CBP's mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies. TECS users collect, maintain, and share information through the TECS Platform to facilitate counterterrorism, law enforcement, border security, and inspection activities. CBP uses this data to assess the risk or threat posed by persons, goods, or conveyances entering or exiting the country.

Law Enforcement and Counterterrorism

TECS users create records on the TECS Platform to document any customs, immigration, or other law enforcement actions taken with respect to a subject, including goods and conveyances, and to document encounters otherwise deemed to be of law enforcement or counterterrorism interest. Certain authorized PGA TECS users create Lookout records to assist CBP's law enforcement and counterterrorism missions at the border by providing information about known or suspected violators or terrorists. For example, certain users from the U.S. Marshals Service enter Lookouts for fugitives into TECS so that a CBP Officer can apprehend the individual at the border.

Authorized PGA TECS users also query individuals and review responsive records in support of their mission. For example, certain authorized users from the FBI access TECS Lookout records to identify individuals suspected of, or involved in, a violation of federal law.

Information-gathering and Assessment

In connection with the counterterrorism DHS Suspicious Activity Reporting Initiative, MOIRs may be reviewed by the CBP Office of Intelligence and the Office of Field Operations. Those MOIRs that meet the necessary criteria for nomination into a Suspicious Activity Report (SAR) are sent to the DHS Information Sharing Environment – Suspicious Activity Report (ISE-SAR) server and further incorporated by DHS as National Security Information (NSI). A detailed description of SARs is discussed in the TECS National SAR Initiative PIA.[42]

[42] DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* www.dhs.gov/privacy.

Benefits Determination

The TECS Platform assists CBP users in making admissibility determinations. Queries are also performed by DHS and partner agencies to evaluate eligibility for their own benefits determination (*e.g.*., USCIS benefit requests, Department of State visa issuance).

Audit Function

CBP uses audit logs to evaluate internal threats posed by trusted users of the TECS community. CBP records and monitors TECS system use and there is no expectation of privacy on the part of any user for any action taken in TECS. The CBP Office of Professional Responsibility (OPR) uses audit logs during the internal investigative process to research claims that TECS users have misused the system. Examples of misuse could include actions such as browsing the system for personal use, or providing operational details to those who might seek unauthorized access to the system or to do harm to CBP or the U.S. Government.

Employee Background Investigations

CBP/OPR queries the TECS Platform for law enforcement data as part of the background investigation process for all applicants and current employees. OPR also uses the TECS platform to suspend mainframe access for current CBP employees who are not in compliance with the reinvestigation requirements. The Office of Information and Technology uses historical background investigation data on the TECS Platform to verify that individuals requesting access to CBP systems have a favorably adjudicated background investigation.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The TECS Platform does not discover predictive patterns or anomalies. TECS only conducts queries for responsive records.

3.3 Are there other DHS components with assigned roles and responsibilities within the system?

Yes. Consistent with DHS regulations and the One DHS policy,[43] CBP shares the information collected in TECS with personnel within all DHS components that have a need-to-know the information, a job function requiring access to the information, and will access data that is consistent with the component's mission.

[43] One DHS Policy, available at, http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

The objectives of sharing TECS data within the DHS community are: 1) to provide the DHS enforcement community with a common repository of information related to suspected or known violators of the law; 2) to provide the ability for timely communication of information related to known or suspected criminals to CBP officers and other DHS employees, such as Immigration and Customs Enforcement agents; and, 3) to provide a common repository for the routine recording of law enforcement activity, including inspection results and assets seized from criminals as a result of law enforcement activities. In addition, TECS provides a repository against which other DHS components can perform queries in support of their specific missions.

CBP and other DHS components are able to access TECS information to perform job functions in conjunction with a need-to-know. A current list of DHS components with access to TECS includes:

- DHS Office of the Chief Security Officer (OCSO)
- DHS Office of the Inspector General (OIG)
- DHS Office of Intelligence and Analysis (I&A)
- DHS Office of Operations Coordination
- National Protection and Programs Directorate (NPPD)
- Transportation Security Administration (TSA), including the Federal Air Marshal Service (FAM)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Secret Service (USSS)

A complete list of the TECS user community can be found in Appendices 2 and 4.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Approximately 90,000 authorized users, including personnel from government agencies outside of CBP and DHS access the TECS Platform for data entry, communication, and data query. There is a risk that TECS could be accessed for unapproved or inappropriate purposes such as searching for, or creating records or Lookouts for friends, relatives, neighbors, the users themselves, or other members of the public.

Mitigation*:* This risk is mitigated through CBP's employment of several layers of training, review, and access controls. All prospective CBP employees and contractors are required to undergo a background investigation before receiving access to TECS; a TECS

account cannot be activated without a properly adjudicated background investigation or change in background investigation status. Additionally, all users must pass an annual TECS Security and Privacy Awareness course in order to establish and retain TECS access. Moreover, TECS users are required to comply with TECS security requirements, including having a supervisor approve a Lookout in order for it to remain on Primary ("on Primary" indicates that immediate action is required by CBP officers if the travelers is encountered crossing the border) in TECS.

CBP OPR continuously monitors the use of TECS, including reviews of the extensive audit logs that TECS maintains, which identifies the users that have accessed records, and what changes or deletions (if any) were made to the records. DHS employees and contractors have no privacy expectations associated with the use of any DHS network, system, or application and this policy is also enforced for TECS. All use of the TECS Platform results in the creation of audit trails designed to document an individual's activity. These audit trails are reviewed in an effort to identify inappropriate uses of the system and misuses of TECS information. All users acknowledge their understanding that their activities within TECS will be monitored, and provide consent to such monitoring each time they log onto the system.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Some information in TECS is collected directly from individuals as they complete primary (and secondary, if applicable) inspection at a port of entry. These individuals have direct notice of the information they provide to the CBP Officers during the admissibility determination process. Some of the information in TECS is collected directly from a suspect after a criminal or administrative arrest. In such cases, the individual is advised in writing and orally of their right to refuse to provide information pursuant to the Fifth Amendment.

With respect to information obtained from suspects or other individuals through Government forms, such as immigration benefit applications, Privacy Act statements on those forms provide notice to the individual that their information may be shared with law enforcement entities.

With respect to Lookout records, or records created during the course of a law enforcement investigation, it is not feasible to provide individuals who are interviewed as suspects, witnesses, or victims with any form of written notice regarding the collection of

information, nor is such written notice required by the Privacy Act or other federal laws or policies. With the exception of authorized undercover operations, however, these individuals are aware that they are being interviewed by a law enforcement officer and that their information is being collected for use in an investigation.

More generally, CBP provides notice through the publication of this PIA, and TECS source system PIAs, SORNs, and implementing regulations associated with individual programs and subsystems that information collected may be shared with other programs and government agencies. CBP also posts signage and video notices at the border explaining what information will be required at Ports of Entry, and publishes this information online at www.cbp.gov.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Generally, the decision of whether to travel to or from the United States is within the discretion of the individual traveler. Pursuant to CBP's authorities, any individual seeking to enter the United States must demonstrate to the satisfaction of the CBP officer that the traveler is a U.S. citizen, lawful permanent resident, or is otherwise eligible for admission to the United States. When applicable, a traveler must also prove he or she is not attempting to import or export any merchandise in violation of U.S. laws. Those unwilling to provide information supporting these requirements can choose not to travel to the United States.

For Lookout or law enforcement records, due to the DHS law enforcement or immigration purposes for which the information is collected, opportunities to decline may be limited or nonexistent. Users may enter data during the course of a law enforcement activity or in support of other DHS proceedings, and it is the nature of the proceeding and the individual rights afforded to the subject by law that will determine the ability of a person to exercise the right to decline to provide information.

There is no opportunity for individuals to decline to provide information that the TECS Platform receives from PGAs via system-to-system interface. However, external agency programs that initially collected the information from individuals may provide them with opportunities to decline to provide their information to that specific program. Opportunities to decline to provide information are enumerated in the program-specific PIA. However, once it has been collected, the data may be shared with TECS as outlined in the collecting system's SORN.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not know that his or her information is being maintained on the TECS Platform.

Mitigation: This risk is mitigated to the extent possible through the publication of this PIA, as well as the publishing of PIAs and SORNs addressing the collection, notification, and

individual control aspects of each subsystem on the TECS Platform. Each PIA describes the data residing on the TECS Platform. With regard to CBP personnel and TECS users, notification that their data resides on the TECS platform is provided on an annual basis when they take the privacy awareness course.

There is a countervailing risk that arises when an individual is notified that information is being collected about them by DHS for a law enforcement or intelligence purpose. The notification may cause the individual to flee or destroy or conceal evidence required by DHS, compromising the ability of DHS agencies to perform their missions, and could put DHS personnel and resources at risk of injury, death, loss, or destruction. In such cases, DHS will intentionally withhold notification to the individual until he or she is arrested or indicted.

Privacy Risk: There is a risk that individuals are not afforded notice or an opportunity to consent to provide information for inclusion in a Lookout or law enforcement record.

Mitigation: This risk can only be partially mitigated. Because the data stored in TECS is used in support of systems in which law enforcement or intelligence contexts apply, notice or the opportunity to consent to use would compromise the ability of the agencies to perform their missions and could put DHS and other law enforcement personnel at risk. Thus, notice of collection and consent to specific uses are limited or not available in most cases for data stored in the TECS However, the methods of providing direct notice as appropriate to an individual are described in Section 6.1 above. There is a potential risk that an individual may not understand the notice. When necessary, the notice to an arrested person is provided in his or her native language through an interpreter or through written translation. There is a potential risk that false or misleading information about an individual may be provided by a source with malicious intent. This risk is mitigated by user training and standard operating procedures that emphasize the importance of verifying information prior to recording and using it.

Section 5.0 Data Retention by the project

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

5.1 Explain how long and for what reason the information is retained.

TECS records are retained for the purposes and durations set out in the SORNs for the various subsystem datasets that reside on the TECS Platform. For example, TECS Lookout records are retained for 75 years from the date of the last collection of data; TECS user information and training records are similarly retained for 75 years, while audit logs are

maintained for 25 years.[44] Lookout records not collected by CBP but residing on the TECS Platform are governed by the owning agency's respective retention policy.

CBP also published SORNs for data collected by the agency that resides on the TECS Platform, including APIS,[45] BCI,[46] NIIS,[47] and SEACATS.[48] Data on these platforms is retained according to the records schedules published in the SORNs.

Datasets not collected by CBP but residing on the TECS Platform include the Non-Federal Entity Data System (NEDS)[49] and the Department of State (DOS) American Citizen Records Query (ACRQ) System.[50] Watchlist records received from the TSC that are included within TECS as a match or possible match to TECS records are maintained for 75 years.

CBP and NARA are reviewing the record retention and disposition schedule for the TECS databases and will update the appropriate SORNs upon completion.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be retained on the TECS Platform longer than is necessary.

Mitigation: This risk is mitigated through CBP's application of data retention policies for the TECS Platform that are consistent with CBP's law enforcement and antiterrorism

[44] DHS/CBP-011, U.S. Customs and Border Protection TECS System of Records Notice, *available at* http://www.dhs.gov/privacy
[45] Information collected in APIS is maintained for a maximum period of twelve months from the date of collection, but may be used to create records in BCI, NIIS, or other systems with differing retention periods.
[46] For U.S. citizens and lawful permanent residents (LPR), BCI will maintain travelers' border crossing information for fifteen years from the date that the traveler was admitted or paroled into the United States. For non-immigrant aliens, to ensure that any information related to a particular border crossing is available for providing any applicable benefits related to immigration or for other law enforcement purposes, the information will be maintained for seventy-five (75) years from the date of admission/parole into the United States. However, for all travelers, BCI records that are linked to active law enforcement activities, and/or investigations will remain accessible beyond the limitations stated above for the life of that activity. *See* BCI SORN.
[47] NIIS data is collected and maintained for seventy five (75) years from the date obtained for purposes of entry screening, admissibility, and benefits determinations. *See* NIIS SORN.
[48] Records related to a law enforcement action; that are linked to an alleged violation of law or regulation, or are matches or suspected matches to enforcement activities, investigations, or cases (i.e., administrative penalty actions or criminal prosecutions), will remain accessible until the conclusion of the law enforcement matter and any other enforcement matters or related investigative, administrative, or judicial action to which it becomes associated plus five years. Records associated with a law enforcement matter, when all applicable statutes of limitation have expired prior to the conclusion of the matter, will be retained for two years following the expiration of the applicable statute of limitations. *See* SEACATS SORN.
[49] NEDS is retained for the duration of the validity of the travel document; that is, 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 DHS/CBP and the issuing authority. *See* Non-Federal Entity Data System.
[50] Retention of records maintained in the DOS ACRQ will vary depending upon when the passport application was received; these documents will be retired or destroyed in accordance with published NARA and DOS record schedules (presently 100 years for electronic records). *See* ACRQ, 73 Fed. Reg. 1660 (Jan. 9, 2008).

missions. Additionally, retention plans are tailored in each subsystem to the particular program needs. TECS provides a systematic evaluation of Lookout Records on Primary to notify the record owner that the "on Primary" designation is about to expire. If the record is not recertified, the record no longer appears "on Primary."

DHS has determined it needs to maintain TECS audit records for a period of 25 years to support internal investigations of TECS misuse and internal threats.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local governments, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. CBP provides access to TECS information for agencies that have the authority to receive TECS data and have demonstrated a justifiable need for this information. The TECS program manager (in concurrence with all necessary DHS/CBP offices) provides authorization for a non-DHS agency's access to TECS via a Memorandum of Agreement (MOA), or other Information Sharing Access Agreement (ISAA), between DHS/CBP and the outside entity. The MOA specifies the general terms and conditions that govern the use of the functionality or data, including privacy-related limitations on use and re-dissemination, and the types of information in TECS to which the agency is being granted access. An Interconnection Security Agreement (ISA) governs any interface implemented between DHS/CBP and that outside entity. For log-in access to TECS, third party agencies must not only identify their authority to receive this information, but also specifically identify and certify an individual(s) that meets TECS employee criteria. Appendices 2, 3, and 4 identify the entities with which CBP shares TECS data, describe what type of TECS data is shared, and how it is shared. CBP has also published PIAs and SORNs which describe the type of data residing on the TECS Platform. *See* Appendix 1.

In the absence of an MOA, TECS data may still be shared with federal, state, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies on a case-by-case basis. In such instances, the requesting or receiving agency must provide a written explanation of (or DHS/CBP must have reason to know) what information the receiving agency needs, how it intends to use that information, and its authority to receive that data. Prior to disclosure, DHS/CBP determines that the proposed use is consistent with a routine use published in the most recent SORN or is otherwise subject to a condition of disclosure under the Privacy Act.

Access to TECS information is governed by need-to-know criteria, which 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 for which it will be employed are the primary privacy-related concerns that are included in the MOA negotiated between DHS/CBP and an agency seeking access to TECS.

Pursuant to the terms of the MOA, authorized PGAs access TECS Platform information through system-to-system connections or as direct users of TECS. Alternatively, if the agency seeking TECS information does not have an electronic interface with TECS, appropriate TECS records may be transmitted pursuant to the terms of an MOA between CBP and the agency or on a case-by-case basis, as discussed above.

Various PGAs and foreign governments connect to TECS for the purposes of law enforcement, screening, and consideration of benefit. Appendix 2 identifies the PGAs and foreign governments that presently have access to TECS and describes the type of data that is being shared.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CBP shares data from the TECS Platform with entities external to DHS in accordance with the Privacy Act exemptions and routine uses identified in the SORNs for the applicable TECS Platform data systems listed in section 1.2. Those routine uses are compatible with the purposes for which those records were collected.

6.3 Does the project place limitations on re-dissemination?

Yes. The use of TECS data outside of DHS is governed by the MOA, which places express limitations on use of CBP data and conditions on re-dissemination, or authorized for narrowly-tailored purposes on a case-by-case basis, as described in Section 6.1. Generally information cannot be re-disseminated without the prior written authorization of CBP. Additionally, agencies accessing information stored on the TECS Platform agree that information not owned by that agency cannot be disclosed by that agency without the specific approval of the agency or entity that owns the records.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The TECS Platform automatically generates a DHS Form 191, *Privacy Act Disclosure Record* whenever a user views TECS Person Subject Records. Case-by-case disclosures are recorded manually on the DHS Form 191 by the CBP or DHS employee making the disclosure. The DHS Form 191 lists: the type of inquiry (written or oral); the name of the subject of the record(s) being sought; the name of the individual, and the associated agency, seeking the

record(s); the address of the requestor; the name of the individual retrieving and providing the records to the requestor; the purpose for the disclosure; the name of the System of Records from which these records are retrieved; a description, in general terms, of the nature of the records provided; and the date of the disclosure. The individual/component maintains a copy of the DHS Form 191 and provides the records to the requestor as well as by the CBP Privacy Office.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be shared under inappropriate circumstances.

Mitigation: This risk is mitigated through CBP's governance of access to datasets on the TECS Platform by need-to-know criteria that demand the receiving entity demonstrate a mission-related purpose for the data before access is granted. Access and use are limited by the initial and ongoing authorization to receive the data, including the negotiation of MOAs between DHS/CBP and the requesting agency. Additionally, to retain TECS access, all TECS users must comply with the TECS security requirements, including successful completion of the TECS Security and Privacy Awareness course on an annual basis. CBP requires PGAs to sign interconnection security agreements before connecting to the TECS Platform to assists in guarding against errant transmissions and misuse.

For all information sharing requests, DHS/CBP reviews the requests for individual records, new user access, and bulk sharing. In the absence of an MOA, TECS data may still be shared with federal, state, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies on a case-by-case basis, as approved by DHS/CBP. In such instances, the requesting or receiving agency must provide a written explanation of (or DHS/CBP must have reason to know) what information the receiving agency needs, how it intends to use that information, and its authority to receive that data. Prior to disclosure, DHS/CBP determines that the proposed use is consistent with a routine use published in the most recent SORN or is otherwise subject to a condition of disclosure under the Privacy Act.

Section 7.0 Redress

The following questions seek information about processes in place for individuals who wish to seek redress (access to records about them, accuracy of the information collected about them, and/or filing complaints).

7.1 What are the procedures that allow individuals to access their information?

DHS has exempted the TECS system of records from access requirements pursuant to 5 U.S.C. § 552a(j) and (k). This is because access to the TECS records could inform a subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. This could enable the individual who is the

subject of a record to impede the investigation, to tamper with witnesses, destroy or conceal evidence, and flee to avoid detection or apprehension.

However, the SORNs for each subsystem governs the access to data in that system – therefore, individuals may be able to access, correct, and amend records from APIS, BCI, or other external agency information. Regardless of exemption, CBP will consider individual requests to determine if information may be released. 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 them by filing a Freedom of Information Act (FOIA) or Privacy Act request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to the CBP FOIA Headquarters Office, U.S. Customs and Border Protection, FOIA Division, 90 K Street NE, 9th Floor, Washington, D.C. 20229. Fax Number: (202) 325-0230.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

A person who believes that CBP actions are the result of incorrect or inaccurate information may request information about their records pursuant to procedures provided by the Freedom of Information Act and the access provisions of the Privacy Act of 1974 by writing to:

U.S. Customs and Border Protection
Freedom of Information Act Division
90 K Street NE, 9th Floor
Washington, D.C. 20229

Travelers may also contact the DHS Traveler Redress Inquiry Program (TRIP) at 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 to identify the record(s) at issue.

7.3 How does the project notify individuals about the procedures for correcting their information?

The TECS Platform does not provide individual notification of procedures for correcting records from each system on the Platform. Instead, notification is set out in those systems' individual SORNs and PIAs. For TECS records that are investigatory in nature, no individual notification is currently provided.

Additionally, CBP Officers provide a Fact Sheet to individuals at ports of entry that outlines the process for correcting data upon request. This fact sheet describes the details in Section 7.2 of this PIA for individuals who believe mistakes in TECS may exist and desire redress. Additionally, DHS Privacy Office published guidance specifically on identifying,

processing, tracking, and reporting on requests for amendments to records submitted to DHS under the Privacy Act.[51]

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know how to request redress related to accessing their records, or with regard to an issue they may have experienced during the customs and immigration inspection process.

Mitigation: To mitigate this risk, CBP has described redress procedures in this PIA as well as the relevant system SORNs. CBP and DHS provide notice to the public of their redress rights on their websites. In addition, as described above, CBP Officers provide a fact sheet to individuals to provide additional information on the process for accessing and correcting records.

Privacy Risk: Due to the law enforcement nature of much of the information in TECS, there is a risk that individuals will be unable to access, correct, or amend their records.

Mitigation: CBP determines all request for redress on a case-by-case basis. If an individual is not satisfied with the response, he or she can appeal his or her case to the appropriate authority provided for in the Privacy Act. There may also be specific legal remedies available to the individual in the context of any criminal or immigration proceedings in which the individual is involved.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The TECS Platform employs a layered approach of checks and balances to ensure information is used in accordance with intended uses stated in this PIA. First, to gain and maintain access to information that resides on the TECS Platform, a user must have the appropriate background investigation and have successfully passed the annual TECS Security and Privacy Awareness course, as well as have a need to know and job-related requirement for TECS information. An agency representative (CBP supervisor or agency National System Control Officer) submits requests to CBP indicating an individual has a need-to-know for official purposes. CBP verifies that background investigations, as well as security and privacy trainings are complete, and issues a new user account upon an affirmative determination.

[51] Privacy Policy Guidance Memorandum 2011-01, *available at* http://www.dhs.gov/privacy-policy-guidance.

The ability to view information within TECS is dependent on both the User Profile assigned to the TECS user, and the access control placed on the information in the database. TECS users consist of CBP/PGA government employees and contractor personnel who are granted only the privileges necessary for them to complete the tasks required as part of their assigned duties. TECS users are generally required to be U.S. citizens who have successfully completed, at a minimum, the appropriate background investigation and have successfully passed the annual TECS Security and Privacy Awareness course, as well as have a need to know TECS information. There are some limited instances where a non-U.S. citizen with a successfully completed and adjudicated background investigation may be granted limited TECS access, following DHS guidelines.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

A new TECS user must complete the TECS Security and Privacy Awareness course and pass the associated test before CBP grants initial TECS access. The course presents Privacy Act responsibilities and Agency policy regarding security, sharing, and safeguarding of official information and PII on the TECS Platform. 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. This training is regularly updated and TECS users are required to take the course annually.

TECS users are educated about the consequences of misuse of TECS records. Inappropriate access to (or use of) TECS can subject a user to criminal and civil penalties, as well as disciplinary actions in accordance with the CBP Code of Conduct to include being removed from one's position.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

TECS users are classified into the following categories: general system users; supervisors; system control officers; systems maintenance personnel; and security administrators. General system users are those CBP and PGA users requiring access to the data stored in TECS. Supervisors are individuals who are responsible for approving records that are added to the system. System Control Officers are responsible for creating and maintaining user provisioning lists. Systems maintenance personnel perform patch management, functionality changes, and testing. Security Administrators are responsible for performing audit reviews.

Every new and existing user of TECS is assigned a system control officer. The system control officer is responsible for the user's profile record and assigns the role(s) (i.e., a CBP

Officer) and the accessible service functions (i.e., Secondary Inspection) within that role. CBP manages the assignment of system control officers so that the system control officer may assign only functions that the system control officer 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. 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.

The TECS platform automatically generates audit logs that capture all users' activity. Audit logs are captured at the time of logon and throughout the user's session. The audit logs consist of a journal of the user's data requests or queries into the TECS datasets, and contain the user ID, date and time, and the location and activity performed, such as the query terms. These audit logs allow system administrators to respond to "user activity" requests from the CBP Office of Professional Responsibility to investigate abuse of the TECS Platform.

Users are required to have and maintain, at minimum, a background investigation status and successfully complete the TECS Security and Privacy Awareness training annually to gain and retain access and certification to information on the TECS Platform. Additionally, TECS users with access to NCIC, Nlets, and the Nlets interface to the CPIC transaction via TECS must be NCIC-certified by successfully completing NCIC testing and certification every two years. The lack of a current certification trumps all other access and is not granted until recertification is complete. Functions required to perform job duties are reinstated after a user completes the recertification.

TECS users can also be assigned a specific transaction on an as-needed basis. A transaction is a collection of capabilities that update, read, or report on data. TECS users must possess both the authority to run the transaction and the authority to read or update the particular record that transaction attempts to access. Typically, transactions are used for temporary assignments and after the temporary assignment is completed, the user profile is reset in order to remove any transaction that is no longer needed. Access through transactions is further limited according to the specific authorization of each user. For example, two users may run the same transaction specifying the same parameters and get two different results if their access permissions differ. Additionally, a user's ability to add a TECS record is limited entirely by the user's role.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Long-standing procedures govern access to, or sharing of, information from the TECS Platform. Information sharing agreements/arrangements are drafted by the CBP operational stakeholders (Office of Field Operations, Office of Border Patrol, etc.) in consultation with the Office of Information Technology program managers. Arrangements that involve PII are sent to the CBP Privacy Officer for review and to DHS for final approval in accordance with procedures developed by the DHS Information Sharing Governance Board.

Responsible Officials

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

John Maulella, Director,
Traveler Entry Programs,
Office of Field Operations,
U.S. Customs and Border Protection
(202) 344-2605

Debra L. Danisek
Acting CBP Privacy Officer
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

Original signed copy of file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix 1. TECS Data and Associated PIAs and SORNs

Sub-system or Interface	Privacy Act – System of Records Notice – Federal Register	Most Recent Published PIA, available at: www.dhs.gov/privacy	General Comments
Sub-systems - Data that resides on the TECS Platform and is collected by CBP			
Advance Passenger Information System (APIS)	73 Fed. Reg. 68435 (Nov. 18, 2008)	DHS/CBP/PIA-001(f) - Advanced Passenger Information System (APIS) Update National Counterterrorism Center (NCTC)	
Border Crossing Information (BCI)	78 Fed. Reg. 31958 (May 28, 2013)	DHS/CBP/PIA-004(h) - Beyond the Border Entry/Exit Program Phase III	
Non-immigrant Information System (NIIS) - I-94 & I-94W data/query	73 Fed. Reg. 77739 (Dec. 19, 2009)	DHS/CBP/PIA-016 - U.S. Customs and Border Protection Form I-94 Automation.	
Seized Asset and Case Tracking System (SEACATS)	73 Fed. Reg. 77764 (Dec. 19, 2008)	DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing	
Data that resides on the TECS but is not collected by CBP			
Interface with U.S. Department of State: American Citizens Record Query System (ACRQ)	73 Fed. Reg 1660 (Jan. 8, 2008)	See Passport Information Electronic Records System PIA (March 1, 2010), *available at* https://foia.state.gov/_docs/PIA/PassportInfoElecRecordsSystems_PIERS.pdf	Passport and related information provided for border patrol, screening, law enforcement, counterterrorism, and fraud prevention activities. ACRQ was formerly the Passport Information Electronic Records System

Sub-system or Interface	Privacy Act – System of Records Notice – Federal Register	Most Recent Published PIA, available at: www.dhs.gov/privacy	General Comments
Interface with Non-Federal Entity Data System (NEDS)	73 Fed. Reg. 43462 (July 25, 2008)	DHS/CBP/PIA-004(e) Procedures for Processing Travel Documents at the Border	Certain States, Native American Tribes, Canadian Provinces and Territories, and other non-Federal Governmental Authorities provide Enhanced Drivers Licenses, Enhanced Tribal Cards, and other identification documents acceptable for travel.
Interface with the DHS Watchlist Service to the FBI Terrorist Screening Center (TSC) Terrorist Screening Database	76 Fed. Reg. 39408 (July 6, 2011)	DHS/ALL/PIA-027(b) Watchlist Service (WLS) Update	In accordance with the Watchlist Service PIA (July 14, 2010), Watchlist information for CBP is maintained in TECS
Data that is accessible through TECS but does not reside on TECS			
Nlets (formerly known as the National Law Enforcement Telecommunications System)	NO	DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing	No SORN because this data is owned by the states of the United States, not subject to Privacy Act
California Law Enforcement Telecommunications System (CLETS)	NO	DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing	See above
Canadian Police Information Center (CPIC)	NO	DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing	No SORN because foreign agencies are not subject to Privacy Act

Appendix 2. TECS Interfaces with Entities External to CBP

Government Agency or Commercial Organization	Remote System Name or Use	TECS Data Type
TECS System-To-System Interfaces with Non-CBP Systems (Inbound)		
Commercial		
ARINC	Carrier APIS determinations	APIS
SITA	Carrier APIS determinations	APIS
Air Carriers	Carrier APIS determinations	APIS
Department of Defense (DoD)		
DoD Personnel Research Center (PERSEREC)	Background checks	Encounter data
Department of Homeland Security (DHS)		
U.S. Immigration and Customs Enforcement (ICE)	Global Enterprise Manager (GEMS), Enforcement Alien Removal Module (EARM), ICE Case Management Modernization Program; Student and Exchange Visitor Information System (SEVIS)	Screening, Lookout
U.S. Secret Service	N/A	Screening, Lookout
Transportation Security Administration (TSA)	Secure Flight, Terrorist Threat Assessment and Credentialing (TTAC), Crew Vetting Program (CVP); used by Office of Investigations (OI)	Lookout
United States Coast Guard (USCG)	APIS determinations	APIS
U.S. Citizenship and Immigration Services (USCIS)	Central Index System (CIS), e-Verify, Alien Documentation, Identification, and Telecommunications System (ADIT), Person-Centric Query System (PCQS)	Travel Documents, Lookout, TECS Screening, Certificates of Eligibility

Government Agency or Commercial Organization	Remote System Name or Use	TECS Data Type
Department of Justice (DoJ)		
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)	Used for firearms & firearm purchase, Lookout creation	TECS Screening, Lookout
Drug Enforcement Administration (DEA)	Narcotics and Dangerous Drugs Information System (NADDIS)	Lookout
Federal Bureau of Investigation (FBI)	International Criminal Police Organization (INTERPOL), National Crime Information Center (NCIC) (person & vehicle), NCIC Interstate Identification Index (III), Terrorist Screening Center (TSC)	APIS, Encounter, TECS Screening, Lookout
Department of Labor	Used for Labor Management Standards	Lookout
Department of State (DoS)		
DoS (Visas)	Immigrant visa transmission from DoS	Travel Documents
DoS (Passport Office)	U.S. passport feed from DoS	Travel Documents
Bureau of Consular Affairs and Office of Diplomatic Security	Consular Lookout and Support System (CLASS)	Lookout
Department of Treasury		
Financial Crimes Enforcement Network (FinCEN)	Case Management Information System (CMIS)	Encounter
State & Local		
International Justice and Public Safety Network (Nlets)	Enhanced Driver's License (EDL) for Michigan, Nlets	Encounter, TECS Screening, Travel Documents, Lookout
California Law Enforcement Telecommunications System (CLETS)	CLETS	TECS Screening
Washington	EDL for Washington	Travel Documents

Government Agency or Commercial Organization	Remote System Name or Use	TECS Data Type
New York	EDL for New York	Travel Documents
Vermont	EDL for Vermont	Travel Documents
Minnesota	EDL for Minnesota	Travel Documents
Pascua Yaqui Tribe	Enhanced Tribal Card	Travel Documents
Kootenai of Idaho	Enhanced Tribal Card	Travel Documents
Seneca Nation	Enhanced Tribal Card	Travel Documents
TECS System-to-System Interfaces with Non-CBP Systems (Outbound)		
Commercial		
ARINC	Carrier APIS determinations	APIS
SITA	Carrier APIS determinations	APIS
Air Carriers	Carrier APIS determinations	APIS
National Insurance Crime Bureau (NICB)	Receipt of vehicle crossing	Encounter (vehicle crossing)
Department of Commerce (DoC)		
Office of Tourism Information (OTI)	Not Provided	Encounter
Department of Defense (DoD)		
DoD PERSEREC	Background checks	Encounter
Department of Homeland Security (DHS)		
DHS Office of Immigration Statistics (OIS)	Not Provided	Encounter
ICE	Student and Exchange Visitor Information System (SEVIS), GEMS, ICE Case Management Modernization	Travel Document, Screening

Government Agency or Commercial Organization	Remote System Name or Use	TECS Data Type
National Protection and Programs Directorate (NPPD)-Office of Biometric Identity Management	Automated Biometric Identification System (IDENT)	APIS, Primary, Secondary, Encounter, Travel Document
TSA	Secure Flight, TTAC, CVP, OI	APIS, Lookout
USCIS	e-Verify, Systematic Alien Verification for Entitlement (SAVE), Computer Linked Application Information Management System (CLAIMS), ADIT, PCQS	Travel Documents (A-Numbers), Encounter, TECS Screening
Department of Justice (DoJ)		
ATF	Support for firearm purchase	TECS Screening
DEA	Use of license plate data	Primary
FBI	Used by Foreign Terrorist Tracking Task Force (FTTTF), INTERPOL, NCIC (person & vehicle), III, & TSC	Encounter, TECS Screening, APIS, Primary, Secondary, Lookout
Department of State (DoS)		
DoS (Passport Office)	U.S. passport feed	Travel documents
Bureau of Consular Affairs and Office of Diplomatic Security	CLASS	Lookout
Department of Treasury		
FinCEN	Supports receipt of Currency & Monetary Instrument Reporting (CMIR) data	Encounter
Other Government Agencies		
Selective Service	not provided	Encounter
State & Local		
Nlets	EDL for Michigan, Nlets	Primary, Secondary, TECS Screening, Travel Documents, Lookout

Government Agency or Commercial Organization	Remote System Name or Use	TECS Data Type
California	CLETS	TECS Screening
New York	EDL	Travel Documents

Appendix 3. TECS Interfaces with CBP Systems

Remote System	TECS Data Type
TECS Interfaces with CBP Systems (Inbound)	
ATS-P	APIS
ATS-P: Lookout Record Creation (Person)	TECS Screening
ATS-P,TF: Immigration Advisory Program (IAP)	Secondary
ATS- P,TF: Integrated Search Service (ISS)	TECS Screening
ATS-TF: Intelligence & Operations Framework System (IOFS)	TECS Screening
ATS-TF: Secured Integrated Government Mainframe Access (SIGMA)	Secondary
ATS-L (Vehicle and Person)	Primary, Secondary, Nlets
Automated Commercial Environment (ACE)	Lookout
TECS Interfaces with CBP Systems (Outbound)	
Office of Field Operations TEC	
Office of Field Operations Management Reporting	APIS, Primary, Secondary
ATS-P	APIS
ATS-P,TF: ISS	TECS Screening
ATS-TF: IOFS	TECS Screening
ATS-TF: SIGMA	Secondary
ATS-L (Vehicle & Person)	Primary, Secondary, Nlets
Enterprise Data Warehouse (EDW)	Encounter
ACE	Lookout

Appendix 4. Partner Government Agencies with Access to TECS

Agency	Sub-Agency
Federal Reserve Board	N/A
Office of the Director of National Intelligence	National Counterterrorism Center
Department of Agriculture	Animal and Plant Health Inspection Service
Department of Commerce	Bureau of Industry and Security
Department of Defense	DOD Office of Inspector General Special Inspector General for Afghanistan Reconstruction
Department of Health and Human Services	Food and Drug Administration
Department of Justice	Alcohol, Tobacco and Firearms Drug Enforcement Administration DEA El Paso Intelligence Center Interpol Federal Bureau of Investigation FBI Information Technology Centers Office of Human Rights and Special Prosecutions Section U.S. Marshals Service
Department of Labor	Office of Labor Management Standards
Department of State	Bureau of Consular Affairs Office of Diplomatic Security
Department of Treasury	Internal Revenue Service (IRS) Financial Crime Enforcement Network (FinCEN) IRS Treasury Inspector General for Tax Administration Bureau of Engraving and Printing Office of Foreign Assets Control Office of Intelligence and Analysis Special Inspector General for Troubled Asset Relief Program

Agency	Sub-Agency
	IRS Criminal Investigations Division Office of Inspector General
Social Security Administration	Office of Inspector General
U.S. Consumer Product Safety Commission	N/A
Department of the Interior	U.S. Fish and Wildlife Service