



# Privacy Impact Assessment

for the

## U.S. Customs and Border Protection Unified Secondary

**DHS Reference No. DHS/CBP/PIA-067**

**December 16, 2020**



**Homeland  
Security**



## Abstract

U.S. Customs and Border Protection (CBP) is tasked with safeguarding America's borders while enhancing the nation's global economic competitiveness by enabling legitimate trade and travel. As part of this mission, CBP conducts inspections of travelers and their belongings at the border. While some travelers are processed during what is referred to as "primary" inspection, others are referred for additional scrutiny, which is a continuation of the border inspection known as "secondary" inspection. This approach enables CBP to facilitate traveler processing. CBP developed Unified Secondary, a module under the Automated Targeting System (ATS), as a consolidated secondary processing system that handles the secondary inspection process from referral to resolution. CBP is conducting this Privacy Impact Assessment (PIA) on the Unified Secondary module because CBP collects, maintains, and disseminates personally identifiable information throughout the secondary inspection process.

## Overview

All persons arriving at a U.S. port of entry (POE) or at a designated pre-clearance location outside the United States are subject to inspection<sup>1</sup> by CBP officers. The initial inspection, also referred to as the "primary" inspection, is generally conducted by a CBP officer who interviews the traveler, inspects travel documents, and uses CBP systems to run basic queries to ensure that (1) the traveler and his or her baggage are admissible; (2) the traveler is not wanted by a law enforcement agency; and (3) the traveler does not pose a health, safety, or national security risk if permitted into the United States. CBP officers at primary have broad discretion to refer travelers for additional scrutiny, commonly known as "secondary inspection," with or without suspicion. Some reasons a traveler will be referred for secondary inspection include: if the CBP officer at primary believes that further inspection is needed; if the officer at primary is alerted to an issue that may require further inspection; to address issues with the documentation or information supplied; or at random. At the secondary inspection location, CBP officers will conduct further assessments to resolve the reason for the referral.

CBP officers use the TECS-based primary system<sup>2</sup> to conduct inspections of travelers entering the United States. Historically, CBP officers have used a TECS subsystem called the Consolidated Secondary Inspection Service (CSIS) to manage referrals of travelers for secondary inspection. CSIS was responsible for transmitting relevant inspection and traveler information it captured to the Secure Integrated Government Mainframe Access (SIGMA), a secondary

---

<sup>1</sup> See 19 C.F.R. § 162.6 Search of persons, baggage, and merchandise, ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.").

<sup>2</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM, DHS/CBP/PIA-009 (2010 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



inspection immigration event management tool and a module of ATS.<sup>3</sup> Unified Secondary is replacing and combining functionality of CSIS and SIGMA into one comprehensive secondary inspection tool. Unified Secondary is housed within the ATS information security boundary.

## Primary Inspection and Referral Process

When travelers present themselves for inspection to a CBP officer, they must first go through the primary inspection process. During this process, the CBP officer inspects the travel documents presented (e.g., passport, visa, enhanced driver's license), requests any relevant information related to the nature of the travel, and collects biometrics on in-scope travelers, as required.<sup>4</sup> CBP also conducts an automatic check of relevant law enforcement systems, including TECS, for any derogatory or other information that may be relevant and support the CBP officer in assessing admissibility. Based on the results of primary inspection, the CBP officer may create a referral in TECS, which indicates a traveler requires additional inspection for issues related to admissibility, customs, baggage, or agriculture.

The primary mission of CBP officers working at primary inspection is to determine whether a traveler and his or her effects are admissible and whether there are any violations of the laws CBP is authorized to enforce or administer at the border. The CBP officer may ask the traveler questions to determine the traveler's purpose and intent for coming to the United States and compare the answers with the travel document and/or type of visa the traveler is using to enter the United States and information in TECS. The CBP officer may also use facial recognition technology to verify the traveler's identity and ensure he or she has presented bona fide travel documents. Additionally, system checks may show the CBP officer if the traveler has had previous encounters with DHS that may impact his or her admissibility.

In addition to determining admissibility and addressing issues relating to border security,

---

<sup>3</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>4</sup> CBP is mandated to biometrically confirm the departure of "in-scope" travelers. An "in-scope" traveler is any person who is required by law to provide biometrics upon exit from the United States pursuant to 8 C.F.R. § 235.1(f)(1)(ii). "In-scope" travelers include "any alien other than aliens exempted under [8 C.F.R. 235.1(f)(1)(iv)] or Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued a form I-94 (see § 1.4) or Form I-95 for admission or parole into the United States." 8 C.F.R. § 235.1(f)(1)(ii). Exempted aliens, pursuant to 8 C.F.R. § 235.1(f)(1)(iv) include, "(A) Aliens younger than 14 or older than 79 on the date of admission; (B) Aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); (C) Classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or (D) An individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply."



during the primary inspection CBP officers are also mandated to guarantee the safe shipment of agricultural and other products into the United States and to keep illicit items out of the United States. Through interviewing a traveler at primary and reviewing his or her travel history and system-generated lookouts and mandatory referrals based upon travel itineraries and previous encounters with DHS, a CBP officer may refer the traveler to secondary inspection for an agricultural or baggage check. For example, a CBP officer may refer a traveler for an agricultural check if a traveler states he or she has recently been to a farm or is bringing in certain food or produce items from certain countries. A CBP officer may also refer a traveler for a baggage check to ensure the traveler is not carrying undeclared dutiable goods or prohibited or restricted items.

CBP creates and uses a variety of methods and techniques to determine whether a traveler should be referred for additional inspection. These include discretionary determinations made based on CBP officer training, knowledge, and experience, including the identification of situations in which there is a question about whether a traveler is using a valid travel document; law enforcement interviewing skills; automated targeting rules to identify travelers and cargo that may merit additional inspection; national security or law enforcement alert lists; and checks against law enforcement or border security lookout records from DHS and other federal agencies.

If the CBP officer creates a referral in the primary inspection system, he or she escorts the traveler to secondary inspection to resolve the referral. Biographic information, any fingerprints or facial images taken during primary inspection, the reason for referral, and CBP officer remarks from primary are automatically transmitted to Unified Secondary from the primary inspection system. Once a referral is made, a CBP officer in secondary will conduct research and interviews and examinations in order to resolve the referral.

A CBP officer at secondary may perform a more in-depth interview or a full inspection relating to issues such as admissibility, customs (baggage), or agricultural, based on the circumstances. During an inspection at secondary, the CBP officer may run law enforcement queries through CBP and other systems on the TECS and/or ATS platform. If the secondary inspection results in a violation being discovered, then a record may also be created in SEACATS.<sup>5</sup>

## Legacy Secondary Inspection Process

Historically, the secondary inspection process relied upon two separate systems: the

---

<sup>5</sup> SEACATS provides CBP with a single repository for enforcement actions related to the Treasury Forfeiture Fund, as well as seized property inventory and case processing information related to arrests, seized and forfeited property, fines, penalties, and liquidated damages. CBP officers document all seizures in SEACATS as an incident report. The incident report may include supporting information about the violation, the property description, quantities of items seized, and information related to the violator. Once an incident report is initiated, the report is assigned a SEACATS number. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE SEIZED ASSETS AND CASE TRACKING SYSTEM, DHS/CBP/PIA-040 (2017), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



Consolidated Secondary Inspection Service (CSIS) and the Secure Integrated Government Mainframe Access (SIGMA).

## CSIS

CBP officers have historically relied on CSIS, a TECS subsystem, to record the results of how the officer resolved the issue that caused the referral to secondary. Biographic information gathered during primary inspection and the reason for referral and the primary officer remarks were transmitted to CSIS from the primary screening system. CBP officers in secondary accessed CSIS to input relevant information obtained during the inspection.

### *Admissibility Referral<sup>6</sup>*

If the inspection result was negative, using CSIS, the officer recorded the following: the type of search conducted, how it was determined there were no issues, results of the inspection, and an indication that the individual was admitted into the United States. If the inspection result was positive, the officer recorded the findings and began an immigration event for the individual in SIGMA.

### *Baggage/Agriculture Referral*

If the inspection result for baggage (customs) or agricultural matters was negative, the officer recorded the results in CSIS, as well as what type of search was conducted and a summary of the inspection, and then released the individual to depart the Federal Inspection Service area. If the inspection result was positive, the officer recorded the results in CSIS and initiated a seizure, penalty, fine, or other enforcement action, which the officer recorded in CSIS and/or another system, such as SEACATS.

## SIGMA

SIGMA, a module of ATS, served two functions in support of CBP secondary inspection operations:

1. An immigration event processing tool for immigration adverse actions and/or administrative action cases.
2. A custody log with a dashboard view of travelers in CBP Office of Field Operations (OFO) custody.

### *Immigration Events*

When an inspection determined that an adverse or administrative immigration action was necessary, the CBP officer began an immigration event. As an immigration events processing tool, SIGMA allowed CBP officers to create immigration events related to secondary inspections. This

---

<sup>6</sup> Additionally, during the admissibility inspection, the secondary officer may discover information related to customs or agriculture issues or other concerns that require additional inspection.



included interview information, the specific legal charges/violations, the final determination of inadmissibility, and other documentation necessary to address admissibility determinations and immigration status. The CBP officer could complete specific forms and documents related to admissibility and immigration status that were added to the traveler's Alien File (A-File) and which noted the inspection and results that led to the CBP officer determination.<sup>7</sup>

### *Custody Management*

CBP also used SIGMA to track and manage inadmissible travelers in custody at a POE. This included identifying the holding location of an individual and information on care offered and provided, such as medical attention given and food and water. When travelers were transferred into the custody of another agency, or returned to their country of origin/residence, that information was also recorded in SIGMA.

### **Secondary Inspection Process with Unified Secondary**

As described above, CBP historically relied on CSIS and SIGMA to complete secondary inspections. CBP is now relying on Unified Secondary to facilitate the secondary inspection workflow by bringing together the functionality of CSIS and SIGMA into a single interface, allowing for more efficient and accurate processing of inspections and immigration events. While Unified Secondary allows CBP officers to complete the majority of the secondary inspection process from one single interface, CSIS and SIGMA will remain as the backend systems that receive inspection information and event, custody, and charging document information, respectively.

Following a referral from primary, Unified Secondary supports the CBP officer through the secondary inspection process by providing prompts for how to document the information obtained during the inspection in order to reach a decision. CBP officers may have to inspect admissibility documentation, baggage, or agricultural products, depending on the reason for the referral. Unified Secondary allows CBP officers to easily access information without having to switch between multiple systems and decreases the amount of duplicative data entry between systems.

Unified Secondary is a consolidated inspection and immigration events processing tool that lists all travelers referred for secondary inspection at a specific port. CBP officers can only view travelers at their assigned duty offices, but certain users with administrative roles can view multiple offices. The referrals queue displays a thumbnail summary view of each traveler referral, which includes: a photograph, taken either at primary or pulled from an existing photograph in CBP

---

<sup>7</sup> Alien Files or "A-Files" are individual files identified by individuals' Alien Registration Number ("A-number"). They contain information regarding the transactions of an individual as they pass through the U.S. immigration process. See DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 78 Fed. Reg. 69983 (September 18, 2017), available at [www.dhs.gov/systems-records-notice-sorns](http://www.dhs.gov/systems-records-notice-sorns).



holdings;<sup>8</sup> biographic information (e.g., name, date of birth, passport number); type of referral (e.g., admissibility, baggage, agriculture); and travel information (e.g., flight number), as well as the status of the traveler in secondary. The CBP officer selects a traveler (either on a first-come, first-served basis or by another method established by the port for workflow efficiency) to begin the inspection, based upon the type of referral.

### Baggage/Agriculture Inspections

The CBP officer or CBP agricultural specialist records the results of a baggage inspection or agriculture inspection in Unified Secondary. As part of the inspection, the officer or agriculture specialist is able to use Unified Secondary to perform record queries of other connected CBP, DHS, and other government agency systems, as listed in Appendix A. For baggage inspections, the CBP officer records the type of examinations performed (e.g., bag examination, person examination, baggage X-ray), the findings of the inspection, and whether the inspection was positive or negative. CBP officers may ask the traveler about the amount of monetary instruments in the traveler's possession and record the information in Unified Secondary. Similarly, for agriculture inspections, the CBP agriculture specialist or officer records the types of examinations performed (e.g., baggage X-ray, baggage examination), the findings of the inspection, and whether the inspection was positive or negative.

For positive baggage/agriculture inspections, the CBP officer or agriculture specialist records information about seizures, fines, or penalties in SEACATS. SEACATS serves as the official record of the seizure, penalty, or liquidated damages. CBP officers create, update, modify, and complete these records within SEACATS. Once the CBP officer creates the SEACATS record, a number is generated in SEACATS. CBP officers record this number with the baggage (or agriculture) inspection in Unified Secondary. The CBP officer may also choose to generate a SEACATS number within Unified Secondary using the referral information from primary inspection. If the CBP officer chooses to generate the number in Unified Secondary, Unified Secondary sends the newly generated number with limited biographic data to SEACATS. The CBP officer can then update, modify, and complete the SEACATS record within SEACATS. The CBP officer (or agriculture specialist) has the ability within Unified Secondary to refer the traveler for additional inspections if something is encountered outside the scope of the inspection being performed, for example if a baggage inspection reveals undeclared meat products.

### Admissibility Inspections

For admissibility referrals, the CBP officer reviews primary inspection remarks and entry documents (such as passports and visas) and conducts an interview, performs systems queries, and if all issues are resolved, admits the traveler. CBP officers record the class of admission and the inspection findings (positive inspection or negative inspection) in Unified Secondary. Unified

---

<sup>8</sup> These photos come from travel documents or previous government in-person encounters with the traveler.



Secondary transmits the data to CSIS (TECS) for storage. For negative inspections, the CBP officer completes the inspection and the traveler is admitted into the United States. The CBP officer may use Unified Secondary to refer the traveler for baggage or agriculture inspection after admission is granted.

## Immigration Events

If the admissibility inspection is positive, the CBP officer completes the inspection and begins an immigration event. The CBP officer takes a sworn statement from the traveler, which is recorded in Unified Secondary. Based on the totality of the circumstances, a disposition is assigned after concurrence from a Supervisory CBP officer. Immigration dispositions could include voluntary withdrawals, expedited removals, or paroles. The CBP officer may complete specific forms and documents related to admissibility and immigration status to be added to the event in Unified Secondary. Secondary inspections that result in adverse or administrative immigration actions are automatically sent to and stored in the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID) as immigration events.<sup>9</sup> EID is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. EID stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, U.S. Citizenship and Immigration Services (USCIS), and CBP. EID supports ICE's processing and removal of aliens from the United States. Future planned functionality for Unified Secondary will involve automating certain notifications to other government agencies and law enforcement partners through Unified Secondary.

## **Form Templates**

For immigration events, as described above, CBP officers may complete forms to document information relating to admissibility and immigration status. In order to streamline this process, Unified Secondary enables a CBP officer to complete a variety of form templates to facilitate and automate required document creation, as well as reducing reliance on paper forms. Depending on the action occurring, from within Unified Secondary a CBP officer will select a document template that will be populated with information available in Unified Secondary. Unified Secondary may also recommend certain forms depending on the specific charges. Once a form is created it can be electronically signed by the CBP officer and, depending on the form, electronically signed by the traveler as well. Completed, signed forms are printed out and placed in the travelers A-File. Depending on the type of document/form, the traveler may be provided a copy of the forms he or she signs. Additionally, the electronic forms are either sent to EID or are

---

<sup>9</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-ice>.





stored in ATS, which are the systems of record for the information, depending on the specific form. Unified Secondary/ATS temporarily maintains a copy of the information on the form so that CBP officers can access information and continue inspection process and investigations in case EID goes offline.

A list of forms in Unified Secondary is available in Appendix B.

## Custody Log

For some individuals for whom CBP opens an immigration event, CBP may hold an individual in custody at a POE until that individual is placed on a return flight or until the individual is turned over to the custody of another law enforcement entity (e.g., ICE) that will repatriate the traveler. For travelers who are held in custody (either awaiting removal or return flight, or waiting to be transferred to another law enforcement agency), CBP maintains a custody log in Unified Secondary. This log provides CBP officers with a consolidated view of all travelers who are being held in custody at a particular POE. This view includes a photograph of the individual, the reason why the individual is being held, and information relating to meals and health and other noteworthy risk factors. CBP officers use the custody log to track people in custody and ensure they are receiving meals, medications, or other necessities as appropriate. CBP officers use Unified Secondary to note when a meal is offered and provided and note any dietary restrictions either for religious or medical reasons. CBP officers can only view the custody log for the POE to which they are assigned.

## System Connections

Unified Secondary is built on the ATS platform; therefore, the source systems available for search via ATS are also available to authorized users via Unified Secondary.<sup>10</sup> In order to streamline the secondary inspection process, Unified Secondary provides CBP officers who have ATS access with the ability to use the ATS search functionality via Unified Secondary to search across CBP, DHS, and other government systems. While these systems have historically been available to CBP officers through multiple user interfaces, Unified Secondary provides a single platform for consolidated searches through existing ATS interfaces. For example, instead of having to open TECS, SEACATS, and USCIS Person Centric Query Service (PCQS)<sup>11</sup> individually, CBP officers can now access those databases by using the super query function in Unified Secondary. However, running a query through the Unified Secondary interface does not provide a CBP officer with access to, or results from, systems the officer does not already have

---

<sup>10</sup> Unified Secondary does not act as the source system for this information and although it may retain a copy of the information in ATS, the majority of this data is sent to the source system of record during the inspection process. The system of record varies depending on the outcome of the inspection.

<sup>11</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



permission to access.

In addition to providing efficient search capabilities, Unified Secondary also allows CBP officers to quickly access other systems using embedded links. CBP officers can link to TECS (to create Inspection Operations Incident Log (IOIL) records), SEACATS (to update search, arrest, seizure (S/A/S) reports), and the CBP Portal (e3) (to capture the traveler's biometrics).<sup>12</sup> Future planned functionality to automate certain notifications to other government agencies through Unified Secondary, such as the FBI when an FBI number is assigned, is not currently available.

A complete list of CBP, DHS, and other government agency systems to which Unified Secondary connects is located in Appendix A.

## 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?

CBP's authority to conduct inspections and detentions at the border is codified in: 8 U.S.C. §§ 1225 and 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, and 1595a(d); 22 U.S.C. § 401; 31 U.S.C. § 5317; the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-456, 118 Stat. 3638); the Tariff Act of 1930, as amended; and the Immigration and Nationality Act ("INA"), codified at 8 U.S.C. § 1101, as well as the attending regulations of CBP promulgated at Titles 8 and 19 of the Code of Federal Regulations.

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

SORN coverage is provided by DHS/CBP-011 TECS, which allows for the collection of information to determine the admissibility of travelers into the United States.<sup>13</sup> Information related to lookouts is also covered by this SORN.

Additional SORN coverage is provided by DHS/CBP-006 Automated Targeting System, which contains information on vetting admissibility and on admissibility determinations.<sup>14</sup> Information related to watchlists is covered by the ATS SORN.

DHS/CBP-013 Seized Assets and Case Tracking System provides SORN coverage for

---

<sup>12</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE, DHS/CBP/PIA-012 (2017 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>13</sup> See DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), available at <https://www.dhs.gov/system-records-notices-sorns>.

<sup>14</sup> See DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), available at <https://www.dhs.gov/system-records-notices-sorns>.



information related to seizures and arrests.<sup>15</sup>

SORN coverage for the information that comes from and goes into A-Files is from DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records.<sup>16</sup>

Information that goes into ICE EID is covered by DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records.<sup>17</sup>

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

Unified Secondary is part of the ATS security authorization boundary, which has undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. ATS received a renewed Authority to Operate on January 15, 2020.

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

Unified Secondary serves as a front-end user interface with a two-way connection to systems to both receive and send data. Unified Secondary receives data from connected systems via ATS and displays it for the CBP officer to use as a part of the secondary inspection process. Unified Secondary only displays data from the connected systems and does not retain it.

CBP officers are able to input data collected during the secondary inspection process for transmission and storage into other systems. For example, information that is sent to TECS is retained for 75 years in accordance with the TECS retention schedule. Many of the forms completed through Unified Secondary are sent to EID as the source system, in which case they are stored for 75 years. Some of the forms generated by Unified Secondary, such as detainee health information, are stored in ATS and retained for 15 years, in accordance with the ATS retention schedule. Information that is entered into SEACATS is stored for the length of the law enforcement investigation plus five years.

---

<sup>15</sup> See DHS/CBP-013 Seized Assets and Case Tracking System, 73 Fed. Reg. 77764 (December 19, 2008), available at [www.dhs.gov/system-records-notices-sorns](http://www.dhs.gov/system-records-notices-sorns).

<sup>16</sup> See *supra* note 7.

<sup>17</sup> See DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (October 19, 2016), available at [www.dhs.gov/system-records-notices-sorns](http://www.dhs.gov/system-records-notices-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.**

Unified Secondary allows CBP officers to create certain immigration forms. All forms CBP officers can create through Unified Secondary are listed in Appendix B, along with the applicable OMB control numbers.

## **Section 2.0 Characterization of the Information**

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

CBP collects and uses a variety of information to refer and resolve secondary inspections. Some of the information is imported from other systems while some information is documented initially through Unified Secondary. While Unified Secondary allows CBP officers to complete the majority of the secondary inspection process from one single interface, CSIS and SIGMA will remain as the backend systems that receive inspection information and event, custody, and charging document information, respectively. Most of the information that is created through Unified Secondary is stored in the systems of record as noted below.

Unified Secondary pushes information to various transactional systems covered by multiple SORNs, depending on the outcome of the inspection. Information about all inspections, both positive and negative, is stored in TECS. Information about agricultural/customs violations is also stored in SEACATS, and information about immigration events is stored in ATS/EID.

Information from TECS collected from travelers at primary inspection, sent to Unified Secondary, and ultimately returned to TECS for storage includes:

- Name (returned to TECS and/or EID);
- Date of birth;
- Gender;
- Citizenship;
- Conveyance used to get to POE;
- Travel document information;
- Birth Certificate (if applicable);
- Driver's License number (if applicable);



- Photograph; and
- Date of Entry.

The following information is documented through Unified Secondary during the secondary inspection and may also be sent to SEACATS:

- Name;
- Date of birth;
- Race;
- Ethnicity;
- Gender;
- Citizenship; and
- Travel document information (type, issued by, number).

The following information is documented through Unified Secondary during the secondary inspection and may also be sent to the system of record for inspections (TECS) and the system of record for immigration events (ATS and if applicable, EID):

- A-File Number (ultimately stored in EID);
- Alias (ultimately stored in TECS and/or EID);
- Race (ultimately stored in TECS and/or EID);
- Complexion (ultimately stored in EID);
- Height (ultimately stored in EID);
- Weight (ultimately stored in EID);
- Hispanic Indicator (ultimately stored in TECS and/or EID);
- Eye and Hair Color (ultimately stored in EID);
- Marital Status (ultimately stored in EID);
- Social Security number (ultimately stored in EID);
- Phone number (ultimately stored in EID);
- Address (ultimately stored in EID);
- Employment (ultimately stored in EID);
- FBI number (ultimately stored in EID);



- Student and Exchange Visitor Information System (SEVIS) ID (ultimately stored in EID);<sup>18</sup>
- Biometrics, captured through separate e3 Biometrics system (Fingerprint Identification Number and photograph) (ultimately stored in IDENT);<sup>19</sup>
- Detainee health information:
  - Free text field which may include information on existing medical conditions, emergent medical conditions, referred for medical assessment (information stays in ATS);
- Disposition (ultimately stored in TECS and/or EID);
- Detainee custody status and location (ultimately stored in EID);
- Welfare checks conducted while in OFO custody (information stays in ATS);
- Juvenile Indicator (ultimately stored in EID);
- If juvenile has a custodian (ultimately stored in EID);
- Names of the family members accompanying the juvenile (information stays in ATS);
- Juvenile separation and reasons for separation (information stays in ATS);
- Relatives (ultimately stored in EID);
- Gang affiliation, if applicable (ultimately stored in EID);
- Class of Admission, if admitted (ultimately stored in TECS and/or EID);
- Arrest date (ultimately stored in EID);
- Status at entry (ultimately stored in EID);

---

<sup>18</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001 (2020), available at <https://www.dhs.gov/privacy-documents-ice>.

<sup>19</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>. DHS is in the process of replacing IDENT with the Homeland Advanced Recognition Technology System (HART) as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about HART, please see U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.



- Event reason (ultimately stored in EID);
- Charge codes selected for prosecution of detainee (ultimately stored in EID);
- Forms listed in Appendix B, which are created through Unified Secondary and are ultimately stored in EID, with the exception of the following forms that are only stored in Unified Secondary/ATS:
  - I-546 – Order to Appear Deferred Inspection;
  - TEDS – Detainee Assessment for Transport Escort, and Detention;
  - Discretionary Authority Checklist for Alien Applicants (Discretionary Checklist);
  - CBP 2500 – Alien Initial Health Interview Questionnaire;
  - I-160 – Notice of Parole/Lookout Intercept; and
  - FD-936 – Request for National DNA Database Entry.

In addition to the specific data elements listed above, Unified Secondary maintains the remarks and/or comments documented by the officer resulting from verbal interviews conducted during the inspection process. This could include information related to the individual's travels, the individual's reasons for entering the United States, and any other information deemed necessary and appropriate by CBP officers for determining admissibility or investigating a potential violation of customs or other U.S. laws enforced by CBP at the border.

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

Information in Unified Secondary comes from a variety of sources and collection methods. Some information is collected during the primary inspection process. Information such as biometrics, travel documentation, or information provided verbally pursuant to an interview may come directly from the traveler. It may also come from information the traveler provided to an agency that shared the information with CBP, such as passport information obtained by CBP from the Department of State (DOS). Additionally, some information in Unified Secondary comes from Advanced Passenger Information (API)<sup>20</sup> and Passenger Name Record (PNR) data that is propagated to ATS. Finally, information may come from agencies, such as from the FBI's National Crime Information Center (NCIC),<sup>21</sup> that provide CBP information without directly receiving it

---

<sup>20</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENER INFORMATION SYSTEM (APIS), DHS/CBP/PIA-001 (2005 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>21</sup> See U.S. DEPARTMENT OF JUSTICE, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL CRIME



from the traveler.

Information in Unified Secondary is also documented during the secondary inspection process. As with information collected at primary, information documented during secondary may come directly from the traveler, such as responses to health or other interview questions. Information may also come from research conducted by the CBP officer through system and open source searches (as outlined on Section 2.3). Additionally, Unified Secondary may include information uncovered during the inspection process, such as information from electronic devices that were searched as part of the inspection.<sup>22</sup>

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

CBP officers may conduct research on travelers using publicly available information, including social media, as part of the inspection process; however, those searches are not conducted using Unified Secondary.<sup>23</sup> LexisNexis® is the only commercial source of data available through Unified Secondary, but data from LexisNexis® is not consistently used as part of the inspection. CBP officer admissibility determinations are based on the totality of the circumstances. If commercial sources or publicly available data are accessed and the information is relevant to the inspection, it is documented in Unified Secondary as part of the inspection and/or immigration event.

### **2.4 Discuss how accuracy of the data is ensured.**

Much of the information documented in Unified Secondary is collected directly from the traveler through his or her documents, including information obtained from the visa application, and the interview. A CBP officer may conduct system queries to determine whether information provided by a traveler is accurate. Through inspections, a CBP officer or agricultural specialist conducts baggage searches to determine if the traveler has contraband or illicit items. CBP may also conduct open source research (outside of Unified Secondary) to ensure travelers are giving accurate statements about their stated activities while in the United States. However, because Unified Secondary is a system used to document inspections referred from primary inspection,

---

INFORMATION CENTER (2019), available at <https://www.fbi.gov/file-repository/pia-ncic.pdf/view>.

<sup>22</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES, DHS/CBP/PIA-008 (2009 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>23</sup> During the secondary inspection process and at the CBP officer's discretion, an officer may conduct open source research to corroborate information that a traveler reveals during the interview portion of the inspection process. This information may be entered into Unified Secondary, to be saved in EID, TECS, or ATS. For more information about how CBP uses social media as part of its screening processes, please see DHS/CBP/PIA-006 Automated Targeting System, *supra* note 3.





false or inaccurate information given to CBP is still maintained in the system because it relates to CBP's secondary inspection of a traveler and may be used to make determinations on how a referral is resolved. Information on travel documents is confirmed through database checks, such as connections to the DOS.

For information available in Unified Secondary that comes from other systems, CBP relies on the accuracy of those systems in maintaining correct information. CBP officers may conduct multiple searches on different data sources to ensure that information in one system is corroborated by other systems. Additionally, some information documented in Unified Secondary is based on CBP officer observations and actions, such as information on medications and meals given to travelers in custody.

## **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** There is a risk that a CBP officer may input inaccurate or false information into Unified Secondary based on inaccurate information provided by the traveler.

**Mitigation:** This risk is partially mitigated. Intentionally providing false information to a CBP officer is a federal offense pursuant to 18 U.S.C. §1001. Information provided by the traveler, including false or inaccurate information, is documented as part of an inspection/immigration event. Admissibility determinations are made based on the totality of the information compiled by the CBP officer and not only the information provided by a traveler.

CBP officers are trained to conduct secondary inspections so that they are able to obtain the most accurate information from the traveler or through other available sources. CBP officers are aware that travelers may lie in order to gain admission or conceal contraband. In order to verify information, CBP officers may conduct baggage searches, query CBP and other government systems, access publicly available information, or order an electronic device search. Inspection results and determinations recorded in Unified Secondary include a totality of the information compiled by the CBP officer and not only the information provided by a traveler. Discrepancies in the information provided by a traveler are mitigated by the information the CBP officer is able to locate from other sources. CBP officers can edit records with accurate information and note when inaccurate information is provided by the traveler. Additionally, travelers are provided the opportunity to review some of the forms created in Unified Secondary and can ask that information be changed if they believe it is incorrect.

**Privacy Risk:** There is a risk that information in CBP systems of record or from other sources may be inaccurate, affecting data integrity in Unified Secondary.

**Mitigation:** This risk is partially mitigated. Unified Secondary is reliant on source systems and external systems, such as LexisNexis®, maintaining accurate information. However, CBP officers may conduct multiple searches on different data sources to ensure that information in one



system is corroborated by other systems. Additionally, some information documented in Unified Secondary is based on CBP officer observations and actions, and those officers have been trained in system use and proper inspection techniques and protocols to identify when inaccurate information is present.

**Privacy Risk:** There is a risk that a CBP officer will enter inaccurate information into Unified Secondary.

**Mitigation:** This risk is mitigated. Manual entry errors are always an inherent risk to any system. However, CBP enabled Unified Secondary to auto populate several data elements from the primary system to ensure that the CBP officer is reviewing accurate information. Additionally, supervisory review is required to review the information prior to a CBP officer making a final disposition on the traveler.

## Section 3.0 Uses of the Information

### 3.1 Describe how and why the project uses the information.

CBP officers use Unified Secondary as an inspection documentation and immigration event management tool. The information recorded in Unified Secondary is the result of inspections performed by CBP officers related to CBP mission responsibilities at the border. Information collected during primary inspection is transmitted to Unified Secondary when an officer creates a referral. The information from the primary inspection is populated from the primary inspection system and displayed in Unified Secondary so the secondary officer may view who the traveler is and the reason why a traveler was referred to secondary inspection. Unified Secondary allows a CBP officer to conduct record queries across CBP systems and other government holdings using a single interface. This reduces the time and potential errors that may come with accessing and querying different systems individually. Once a CBP officer completes the document review, traveler interview, system queries, and baggage inspection (as applicable), the officer makes a determination and records the class of admission and the inspection findings (positive inspection or negative inspection) in Unified Secondary. For certain positive inspections where additional action is required, such as a seizure of goods, the officer inputs information into other CBP systems. If a CBP officer determines a traveler is inadmissible, the CBP officer completes the inspection and begins an immigration event in Unified Secondary. For the event, the CBP officer sets a disposition, enters charges, and completes specific forms and documents necessary for removal or other immigration action. Once the secondary inspection is completed, Unified Secondary sends the outcome of the inspection to the appropriate system of record for retention. All inspections, both positive and negative, are sent to TECS, and immigration events are sent to ATS/EID.<sup>24</sup>

---

<sup>24</sup> Unlike TECS, ATS, and EID, Unified Secondary does not send the outcome of the inspection/violation to SEACATS. CBP officers must complete these violations in SEACATS. The only information sent from Unified



In addition to documentation of inspection results and immigration event management, Unified Secondary maintains a custody log for travelers who are held in custody (either awaiting removal or return flight or waiting to be transferred to law enforcement). This log provides CBP officers with a consolidated view of all travelers who are being held in custody in a particular POE. CBP officers use the custody log to track where the traveler is located within the port; the conditions where the traveler is located to ensure he or she is safe and sanitary; and that travelers are receiving meals, medications, or other necessities as appropriate. The custody logs allow for continuity during shift changes to ensure the health, safety, and wellbeing of those in CBP custody.

### **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. Unified Secondary does not analyze any data in the database for purposes of discovering or locating a predictive pattern or an anomaly.

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

Only CBP personnel have roles and responsibilities in Unified Secondary. However, other entities are able to create TECS lookouts that, when hit on during primary inspection, send travelers to secondary inspection. If the hit is for criminal activity, CBP may hold a traveler in custody until the custody of the traveler is turned over to the other law enforcement agency.

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** Authorized users of Unified Secondary could use their access for unapproved purposes.

**Mitigation:** This risk is mitigated. In order to become an authorized user, personnel must successfully complete privacy training and hold a full background investigation clearance. A user must also have a job-related requirement to access the specific information. Additionally, because Unified Secondary will use some aspects of the TECS platform, all users of Unified Secondary are required to complete and pass an annual TECS Privacy Act Awareness Course to maintain their access to the system. The training course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to TECS and affiliated TECS platform and the

---

Secondary to SEACATS is the data necessary to generate the SEACATS number.



training is regularly updated.

To further mitigate the risk of misuse of information by CBP personnel with access to Unified Secondary, access to data in Unified Secondary is controlled through passwords and the use of personal identity verification (PIV) cards issued to federal employees which assures the appropriate level of security and access to information systems as well as restrictive rules pertaining to user rights. Users are limited to roles that define authorized use of the system. For example, access can be limited to the specific POE where a CBP officer works and the CBP officer will be unable to view referrals for other ports of entry. Management oversight is in place to ensure appropriate assignment of roles and access to information.

Finally, audit logs capture the activity of a user accessing Unified Secondary, 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. Audits are conducted to log all privileged user transactions and monitor for abuse. These audit logs monitor user's keystrokes and access sessions for purposes of ensuring compliance with the safeguarding and security protocols.

**Privacy Risk:** There is a risk that information documented in Unified Secondary will be shared or used inappropriately within the Department.

**Mitigation:** This risk is mitigated. Only CBP personnel have access to Unified Secondary. In order to become an authorized user, personnel must successfully complete privacy training, hold a full background investigation clearance, and have a job-related requirement to access the specific information. Additionally, because Unified Secondary will use some aspects of the TECS platform, all users of Unified Secondary are required to complete and pass an annual TECS Privacy Act Awareness Course which includes Privacy Act responsibilities and agency policy with regard to sharing. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy.

To further mitigate the risk of improper sharing, access to data in Unified Secondary is controlled through passwords and the use of PIV cards as well as restrictive rules pertaining to user rights. Audit logs also capture the activity of a user accessing Unified Secondary, including user identifier, date, time, and location of the access, as well as the type of activity performed.

## Section 4.0 Notice

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

CBP maintains signage throughout the primary and secondary inspection areas that inform travelers on inspections and collection of information. This PIA, as well as the TECS Primary and Secondary PIA and the TECS SORN, also provides notice of collection. The ATS and SEACATS



PIAs and SORNs provide additional notice.

CBP provides travelers notice for information collected on forms by allowing travelers to complete or review a form and then provide their signature. Additionally, CBP officers provide verbal notice about the purpose of the form and use of the collection of information. CBP may also provide travelers with a tear sheet explaining the Freedom of Information Act (FOIA) process if travelers wish to request information about their interaction with CBP. Additional tear sheets provide travelers with information on the inspection of electronic devices<sup>25</sup> and personal searches. Additionally, some of the information in Unified Secondary comes from other systems, in which cases CBP relies on the source of the collection for notice.

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

International travel is voluntary, but travelers referred for secondary inspection do not have the ability to opt out of secondary inspection. As Unified Secondary is the case management system for secondary inspection, travelers also do not have the ability to opt out of having their information included in Unified Secondary. CBP cannot require travelers to provide information during secondary, but failure to provide information may result in a traveler being found inadmissible or may delay the individual's travels while CBP tries to find answers and verify information through other methods previously outlined in this document. CBP provides notice about the effect not providing information may have on travel plans via the posted signage.

## **4.3 Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** There is a risk that travelers will not know what information is used to make admissibility determination and other secondary inspection resolutions.

**Mitigation:** This risk is mitigated. This PIA serves as notice of the information CBP collects to make admissibility determination and other secondary inspection resolutions. Much of the information documented in Unified Secondary is gathered directly from the traveler during the interview. CBP officer questions inform the traveler what information CBP officers are concerned about and considering when making determinations.

## **Section 5.0 Data Retention by the Project**

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

Unified Secondary serves as a front-end user interface with a two-way connection to

---

<sup>25</sup> See *supra* note 22. The CBP Border Searches of Electronic Devices PIA provides additional notice of the electronic border search process and the authority under which CBP conducts those searches. An example of a CBP tear sheet can be found here: see <https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf>.



systems to both receive and send data to. Unified Secondary receives data from connected systems via ATS and displays it for the CBP officer to use as a part of the secondary inspection process. Unified Secondary only displays data from the connected systems and does not retain it.

CBP officers are able to input data collected during the secondary inspection process into Unified Secondary for transmission and storage into other systems, where it is retained in accordance with the retention schedules for those systems. For example, information that is sent TECS is retained for 75 years in accordance with the TECS retention schedule. Many of the forms completed through Unified Secondary are sent to EID as the source system, in which case they are stored for 75 years. Some of the forms generated by Unified Secondary, such as detainee health information, are stored in ATS and retained for 15 years, in accordance with the ATS retention schedule. Information that is entered into SEACATS is stored for the length of the law enforcement investigation plus five years. For information that is included in an official A-File, records are retained permanently, consistent with the A-File SORN. The official A-File record may take three possible forms: (1) records contained within the paper A-File; (2) records contained within the electronic record from USCIS Enterprise Document Management System (EDMS)<sup>26</sup> or USCIS Electronic Immigration System (ELIS);<sup>27</sup> or (3) a combination of paper and electronic records and supporting documentation. A-File records are maintained in accordance with N1-566-08-11. DHS/USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is the risk that, due to the variety of source systems that feed information into Unified Secondary, the information will be kept or deleted in a manner inconsistent with the source system retention.

**Mitigation:** This risk is mitigated. As an inspection documentation and immigration event management tool, Unified Secondary retrieves information from other source systems for use by the CBP officer and/or agricultural specialist and populates information inputted by the officer and/or specialist into the respective system of record once the inspection is complete. Information retrieved by the officer is displayed via Unified Secondary but continues to reside in the source system. Unified Secondary retrieves information from the source system in real-time, to ensure the CBP officer is accessing the most up-to-date information.

Unified Secondary also sends information to the appropriate system for storage. The

---

<sup>26</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT SYSTEM, DHS/USCIS/PIA-003 (2007 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

<sup>27</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC INFORMATION SYSTEM, DHS/USCIS/PIA-056 (2018 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



system and length of retention varies based on the outcome of the inspection to the appropriate system of record for retention – positive/negative inspections (75 years in TECS), immigration events (15 years in ATS), and adverse actions (75 years in EID).

## Section 6.0 Information Sharing

### **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.**

Information collected through Unified Secondary is shared on a case-by-case basis with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, or when CBP believes the information would assist enforcement of civil or criminal laws. Unified Secondary pushes information to various transactional systems covered by multiple SORNs; all sharing is done according to the appropriate system of record.

As an example, Unified Secondary maintains a direct interface with the U.S. State Department Consular Consolidated Database (CCD)<sup>28</sup> by which data from Form I-275, Notice of Visa Cancellation/Border Crossing Card Voidance, is transmitted directly from Unified Secondary to CCD so that the State Department can cancel the Visa or Border Crossing card within CCD to ensure that future travel does not occur under the cancelled travel document.

DHS counterterrorism, law enforcement, and public security communities may be provided with information about suspected or known violators of the law and other persons of concern identified through secondary inspections documented in Unified Secondary. CBP may share the inspection information documented in Unified Secondary with other components within DHS when there is a need-to-know in accordance with their official responsibilities, including collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. This sharing is through the system of record, for example TECS.

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

CBP will share information documented in Unified Secondary with external organizations consistent with the published routine uses in the SORNs that cover Unified Secondary (listed in Section 1.2), which are compatible with the original purpose of collection. In the event that CBP

---

<sup>28</sup> See U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (2018), available at <https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf>.



shares information documented in Unified Secondary outside of CBP, CBP will detail the established data sharing practices in Memoranda of Understanding/Agreement (MOU/A) and Interconnection Security Agreements (ISA), when appropriate, which govern the sharing of information documented in Unified Secondary and residing in ATS or TECS. Under the terms of these MOUs and ISAs, other agencies will secure Unified Secondary information consistent with approved security practices that meet DHS standards. Recipients from other agencies will be required by the terms of the information sharing agreement to employ security features to safeguard the shared information.

### **6.3 Does the project place limitations on re-dissemination?**

Yes. CBP enters into MOU/As with external organizations prior to the systematic sharing of information. When sharing information with parties outside of CBP, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for CBP are applied to the outside entity. Any agreements between CBP and external entities fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing.

Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, CBP includes justification for collecting the data and an acknowledgement that the receiving agency will not share the information without CBP's permission, as applicable.

Information that is shared with other agencies, federal, state, local, tribal or foreign, outside of the context of any MOU/A or prior written agreement generally requires a written request by the requesting agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office.

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

MOU/As and other written agreements defining roles and responsibilities are executed between CBP and each agency that receives data documented in Unified Secondary on a systematic basis. The information may be transmitted either electronically or as printed materials to authorized personnel. Electronic communication with other non-CBP systems may be enabled via message/query-based protocols delivered and received over secure point-to-point network connections between CBP systems and the non-CBP system. CBP's external sharing of the data recorded in Unified Secondary complies with statutory requirements for national security and law enforcement systems.

Information that is shared with other agencies, federal, state, local, tribal, or foreign,





outside of the context of any MOU/A or other prior written arrangement generally requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office and documented in DHS Form 191.

## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk that information documented in Unified Secondary will be inappropriately shared to external partners.

**Mitigation:** This risk is partially mitigated. When sharing information that is collected by Unified Secondary with parties outside of DHS, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to Unified Secondary records is governed by a need-to-know criterion that demands the receiving entity demonstrate the mission-related need for the data before access is granted. The reason for the access, a specific mission purpose, and an intended use consistent with the receiving agency's purpose and CBP's justification for collecting the data are also concerns that are included in either the terms of a negotiated MOU/A and ISA or the language of an authorization providing facilitated access to an external agency. The MOU/A specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. The ISA specifies the data elements, format, and interface type, including the operational considerations of the interface. MOU/As and ISAs are periodically reviewed, and outside entities must agree to use, security, and privacy standards before sharing can continue.

**Privacy Risk:** There is a risk that information documented in Unified Secondary will be shared inappropriately within the Department.

**Mitigation:** This risk is mitigated. Only CBP personnel have access to Unified Secondary. In order to become an authorized user, personnel must successfully complete privacy training, hold a full background investigation clearance, and have a job-related requirement to access the specific information. Additionally, because Unified Secondary will use some aspects of the TECS platform, all users of Unified Secondary are required to complete and pass an annual TECS Privacy Act Awareness Course which includes Privacy Act responsibilities and agency policy with regard to sharing. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy.

To further mitigate the risk of improper sharing, access to data in Unified Secondary is controlled through passwords and the use of PIV cards as well as restrictive rules pertaining to user rights. Audit logs also capture the activity of a user accessing Unified Secondary, including user identifier, date, time, and location of the access, as well as the type of activity performed.



## Section 7.0 Redress

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

Individuals seeking notification of and access to information contained in TECS or ATS, or seeking further information related to their secondary inspection, may gain access to certain information by filing a FOIA request with CBP at <https://foia.cbp.gov/palMain.aspx>, or by mailing a request to:

U.S. Customs and Border Protection (CBP)  
Freedom of Information Act (FOIA) Division  
1300 Pennsylvania Avenue NW, Room 3.3D  
Washington, D.C. 20229  
Fax Number: (202) 325-1476

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information.

All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

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

Individuals are able to correct inaccurate or erroneous information in Unified Secondary throughout the secondary inspection process. Individuals can inform CBP officers of inaccurate information if CBP officers ask them a question containing inaccurate information about them. In addition, individuals are able to review and sign some of the forms created in Unified Secondary and they can inform CBP officers of any inaccurate information in the forms.

A person who believes that CBP's actions are the result of incorrect or inaccurate information may request information about his or her records pursuant to procedures provided by FOIA. U.S. citizens, lawful permanent residents, and individuals who have records covered under the JRA who believe that CBP's actions are the result of incorrect or inaccurate information may request correction of that data under the amendment provisions of the Privacy Act of 1974 by writing to the above address. The CBP Privacy Division reviews all requests for correction and amendment regardless of status.



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](http://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?**

Individuals are notified of the procedures for correcting their information through the SORNs describing each of the underlying systems from which Unified Secondary accesses information. This PIA also serves as notification. Additionally, signage and tear sheets at ports of entry provide information on how to contact the DHS TRIP. In addition, travelers may request information from the on-site CBP officer.

### **7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** There is a risk that travelers will not know how to request redress.

**Mitigation:** This risk is partially mitigated. This PIA provides information on how to request access and amendments to information documented in Unified Secondary. Additionally, CBP officers inform travelers verbally and through tear sheets on how they can challenge a determination and request information CBP used to make a determination. Travelers who wish to access information about themselves or challenge a determination can submit a FOIA request to CBP or a TRIP request to the Transportation Security Administration (TSA) via the addresses above. Additionally, U.S. citizens, lawful permanent residents, and individuals covered by the JRA, may submit a Privacy Act Amendment request to CBP.

## **Section 8.0 Auditing and Accountability**

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

Access to the system is limited to internal CBP users. System access is not provided to non-CBP personnel. Access is limited to those personnel with a job-related requirement to access the information. All users with access to the system are required to have full background checks. In addition to access to Unified Secondary, CBP personnel will also need separate access to the systems that provide information that can be queried in Unified Secondary.

Users of Unified Secondary will be assigned different privileges based on their positions and roles to carry out their official duties. Audits will be conducted to log all privileged user transactions and monitor for abuse.

In addition, rules of behavior are established for each major application, including Unified Secondary. These rules of behavior require users to be adequately trained with regard to the



security of their systems. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. All CBP system users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. The rules of behavior already in effect for each of the component systems from which Unified Secondary draws information will be applied to the program, adding an additional layer of security protection. Security, including access-related controls, will be certified initially and at specified intervals through the Security Authorization Process of the Unified Secondary system.

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

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

CBP employees are also required to sign statements acknowledging that they have been trained and understand the security aspects of their systems and comply with the following requirements:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and Unified Secondary policies and procedures.

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

The personally identifiable information documented in Unified Secondary will be accessed primarily by CBP officers working at a POE or preclearance location. Unified Secondary has provisions and roles to determine what access is provided to users. CBP is able to limit what ports a user views so that they are only able to see the travelers waiting for inspection at their current port and not all travelers across the country. Additionally, users have to be separately provisioned to access the source systems that feed into Unified Secondary in order to view that information documented in Unified Secondary.



## **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?**

Any information sharing agreements for this data will define the nature of access, the scope of information subject to the sharing agreement, and the privacy, security, safeguarding, and other requirements. All information sharing arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

### **Contact Official**

Emilia Bakopoulos  
Director, Systems Enforcement Analysis and Review Division  
Admissibility and Passenger Programs  
Office of Field Operations  
U.S. Customs and Border Protection  
(202) 344-1372

### **Responsible Official**

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

### **Approval Signature**

[Original copy signed and on file with the DHS Privacy Office]

Dena Kozanas  
Chief Privacy Officer  
U.S. Department of Homeland Security  
(202) 343-1717



## Appendix A

### Unified Secondary System and Program Connections

CBP officers can use Unified Secondary to view information from a variety of systems. Unified Secondary does not ingest the information from these systems but rather accesses the data tables stored in ATS or TECS. CBP officers are also able to write information directly to some systems through Unified Secondary. At this point, the only external system Unified Secondary can send information to is DOS CCD. In the future, CBP plans to update Unified Secondary to connect to other non-DHS systems. However, CBP officers may query and view information from the following systems via Unified Secondary:

DHS Systems and Programs		
System/Program	DHS System Owner	Reason for Access
Advance Traveler Information System (ATIS)	CBP	ATIS serves as the back-end system that transfers and stores information from front-facing systems to appropriate systems for vetting and validation. CBP officers take a new photograph using Simplified Arrival, as part of the primary inspection process. As part of the Advance Travel Authorization (ATA) process and consistent with CBP policy, these noncitizens are then referred to secondary inspection for further processing. As part of the secondary inspection for the ATA process, the CBP officer will see a 1:1 photo match score on the ATA application. This 1:1 photo tool is available to secondary as part of an OFO requirement. This enhancement may use the 1:1 photo comparison tool within USEC to compares the previously submitted CBP One photo to the photo from primary processing. USEC sends the CBP One and Simplified Arrival photograph to TVS who then responds with a match score on a scale of 0-10000. This photo comparison is a tool for officers to help determine if the noncitizen who submitted the ATA application is the same noncitizen who arrived at the POE.
Analytical Framework for Intelligence (AFI) <sup>29</sup>	CBP	AFI is a CBP system that includes intelligence reports on travelers of interest. CBP officers use this information to verify traveler information and inform questioning. CBP officers can view and query this information through Unified Secondary, but cannot send information to AFI.

<sup>29</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE, DHS/CBP/PIA-010 (2012 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



Arrival Departure Information System (ADIS) <sup>30</sup>	CBP	ADIS is a person centric system showing overstay information and previous travel and it assists CBP officers in questioning travelers. Through Unified Secondary, CBP officers can query and view records in ADIS but not directly send information to ADIS. An I-94 completed through Unified Secondary would update in ADIS.
APIS (U.S. Nexus and Foreign APIS) <sup>31</sup>	CBP	APIS information is used by CBP officers to research previous travel and inform them on questions to ask travelers and any concerning travel patterns. Through Unified Secondary, CBP officers can query and view records in APIS but cannot send information to APIS.
Case Acceptance System (CAS)	ICE	CAS was developed by ICE to streamline the transfer of individuals from CBP custody into ICE custody. CAS enables CBP to provide ICE with real-time notifications, upon completion of CBP's processing of encountered individuals. Once an ICE-ERO officer knows CBP has completed a case, the ICE-ERO officer will use CAS to view the applicable records as well as the forms available in the Unified Immigration Portal (UIP).
Central Index System (CIS) <sup>32</sup>	USCIS	CIS is a U.S. Citizenship and Immigration Services system that shows the immigration status of individuals. It is used by CBP officers to verify status. Through Unified Secondary, CBP officers can query and view information in CIS, but they cannot send information to CIS.
Currency and Monetary Instrument Report (CMIR) <sup>33</sup>	CBP	CMIR is TECS subsystem that collects information on the export and import of monetary instruments greater than \$10,000. This information is used by CBP officers to inform their questioning and verify that the CMIR form submitted by the traveler is accurate. CBP officers are able to query and view but cannot send information to CMIR via Unified Secondary.
DOMEX <sup>34</sup>	CBP	DOMEX is an ATS data source containing information retrieved from electronic devices. CBP officers use DOMEX to identify connections between the traveler and persons of

<sup>30</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM, DHS/CBP/PIA-024 (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>31</sup> See *supra* note 20.

<sup>32</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM, DHS/USCIS/PIA-009 (2007 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

<sup>33</sup> See *supra* note 2.

<sup>34</sup> See *supra* note 3.



		interest and to inform questioning. CBP officers are only able to query and view DOMEX information in Unified Secondary, not send information to DOMEX.
Electronic Media Records (EMR)	CBP	EMR is used to keep a record of Electronic Media Reports conducted in the secondary inspection process. As an extension of the secondary inspection process, the system provides EMR users the capability to keep track of all electronic media items (e.g., mobile phones, computers, laptops, CD/DVD media, USB drives) that are confiscated during secondary inspection or abandoned. EMR helps detect evidence relating to terrorism and other national security matters, (e.g., human, and bulk cash smuggling, contraband, and child pornography). This examination can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations.
Electronic System for Travel Authorization (ESTA) <sup>35</sup>	CBP	ESTA is a CBP system used to determine whether citizens and nationals of Visa Waiver Program countries are eligible travel to the United States. CBP officers use this information to review answers provided by the traveler in order to ensure accuracy or conduct further questioning or research. CBP officers are able to query and view but cannot send information to ESTA via Unified Secondary.
Electronic Visa Update System (EVUS) <sup>36</sup>	CBP	EVUS is similar to ESTA and CBP officers use the information provided by the traveler to inform questioning and conduct research. Through Unified Secondary, CBP officers are able to query and view, but cannot send information to this system.
Enforcement Integrated Database (EID) <sup>37</sup>	ICE	EID is an ICE system that operates as a repository of information on people encountered during immigration investigations. CBP officers use this information to determine whether the traveler has had adverse action taken against them previously and to vet information provided by the traveler. CBP officers are able to query and view and send information to EID. All forms completed by CBP

<sup>35</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>36</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC VISA UPDATE SYSTEM, DHS/CBP/PIA-033 (2016), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>37</sup> See *supra* note 9.





		officers are transferred to EID as the source system of the records.
Foreign Encounters (Biometric Identification Transnational Migration Alert Program (BITMAP), Secure Real-Time Platform (SRTP)) <sup>38</sup>	ICE	This information allows CBP officers to access biographic and biometric information on foreign travelers and verify information. BITMAP is an ICE-owned System and SRTP is owned by DHS.
I-94 <sup>39</sup>	CBP	I-94 information is used to verify travel as well as determine previous overstay information. The I-94 also contains information on the traveler's activities during travel and is used to inform questioning. CBP officers are able to query, view, and create I-94s through Unified Secondary.
IDENT <sup>40</sup>	OBIM	IDENT contains biometric information on travelers. CBP officers use this information to verify identity. CBP officers can submit biometric information to IDENT as well as query and view IDENT records using Unified Secondary.
Intelligence Reporting System (IRS) <sup>41</sup>	CBP	CBP officers review information in IRS in order to view any intelligence and informational reports on the traveler to determine admissibility and inform questioning. Through Unified Secondary, CBP officers are able to query and view, but cannot send information to this system.
Master Crew List (MCL) <sup>42</sup>	TSA/CBP	MCL contains information on crew that is used to verify information given to CBP officers and inform questioning. This information comes from ATS. Through Unified Secondary, CBP officers are able to query and view, but cannot send information to MCL.

<sup>38</sup> DHS is currently developing a PIA for this sharing initiative. It will be made available at <https://www.dhs.gov/privacy-impact-assessments>.

<sup>39</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE I-94 WEBSITE APPLICATION, DHS/CBP/PIA-016 (2013 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

<sup>40</sup> See *supra* note 19.

<sup>41</sup> CBP is currently developing a PIA to describe this system. However, see DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44198 (September 21, 2017), available at [www.dhs.gov/systems-records-notices-sorns](http://www.dhs.gov/systems-records-notices-sorns).

<sup>42</sup> See *supra* note 3.



Passenger Name Records (PNR) <sup>43</sup>	CBP	PNR information is provided by the airlines and is used by CBP officers to conduct research, vet information, and inform questioning. PNR information is located in ATS.
SEACATS <sup>44</sup>	CBP	SEACATS contains a record of all CBP seizures and arrests. CBP officers use this information to see if a traveler has previously been arrested by CBP or traveled with an item that was later seized. CBP officers can view, query, and write to SEACATS. Information from Unified Secondary can be ported over to SEACATS if a CBP officer determines that a seizure or arrest will be made.
Student and Exchange Visitor Information System (SEVIS) <sup>45</sup>	ICE	SEVIS is an ICE system that contains information on and related to nonimmigrant students. This information is used by CBP officers to conduct research and inform questions. Through Unified Secondary, CBP officers are able to query and view, but cannot send information to this system.
TECS Lookout Records <sup>46</sup>	CBP	Lookout records are created by CBP officers and other agencies with TECS access to inform CBP officers at primary that a traveler may need to be referred for secondary inspection. CBP officers in secondary use this information to understand why a traveler was referred, to contact the individual who placed the lookout, and to inform questioning. CBP officers can view, query, and create Lookout Records through Unified Secondary.
Trusted Travelers <sup>47</sup>	CBP	CBP administers Trusted Traveler programs in which qualified individuals are eligible for designated screening at Ports of Entry. CBP officers use this information to verify traveler information and inform questioning. Trusted Traveler information is housed in the Global Enrollment System (GES) and sends a copy to ATS. CBP officers can only query and view Trusted Traveler information. CBP officers cannot send information to GES through Unified Secondary

<sup>43</sup> See *supra* note 3.

<sup>44</sup> See *supra* note 5.

<sup>45</sup> See *supra* note 18.

<sup>46</sup> See *supra* note 2.

<sup>47</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE GLOBAL ENROLLMENT SYSTEM, DHS/CBP/PIA-002 (2006 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



TSA Overflight and Foreign to Foreign <sup>48</sup>	TSA	This system provides information on flights and travelers that fly over the United States. CBP officers use this information to verify traveler information and inform questioning. CBP officers can view and query this information through Unified Secondary but cannot send information to this system.
Unified Immigration Portal (UIP)	CBP	UIP is a visualization tool that provides a single interface for data sources from certain agencies involved in the immigration lifecycle to enable a more complete understanding of an individual's immigration journey. USEC sends data to UIP, which is viewable by partner agencies.

<b>Non-DHS Systems and Programs</b>	
<b>System/Program</b>	<b>Reason for Access</b>
Canadian Land Border Entry Records	This information is available in ATS via a TECS connection with the Canadian Border Services Agency (CBSA). CBP officers use the information to verify travel. The CBSA owns the information in this system.
Consular Electronic Application Center (CEAC)	This information is available in ATS via a direct connection with the Department of State (DOS). This data source includes information used by nonimmigrant and immigrant visa applicants to apply for a visa. CBP officers use this information to verify traveler provided information and inform questioning. The DOS owns information in this system.
Consular Consolidated Database (CCD)	Consular Consolidated Database is a DOS system that contains visa and passport information. CBP officers use this information to verify information and conduct research. Through a direct connection, CBP officers can recommend that a visa be revoked. The DOS owns information in this system.
National Crime Information Center (NCIC)/Interstate Identification Index (III)/ National Law Enforcement Telecommunications System (Nlets)	Information on warrants found in NCIC/III is available through a connection in TECS. This information is used to refer travelers to secondary and CBP officers in secondary will use the information to determine whether the traveler needs to be held in custody on the warrant awaiting pick up by the entity that obtained the warrant. CBP officers may also conduct research based on this information. The FBI owns NCIC and III information. Nlets information is owned by Nlets, a private corporation owned by the states that participate in the data exchange network.
Interpol	Interpol queries allow officers to view whether a passport has been reported lost or stolen. CBP officers use this information to conduct research and inform questioning, and may contact Interpol for further information on a traveler.

<sup>48</sup> See *supra* note 3.



LexisNexis®	LexisNexis® is a commercial product providing access to court records and other public documents on an individual. CBP officers use this information to conduct research, inform questioning, and verify information. LexisNexis® is a product provided by a company of the same name which is owned by RELX, a publicly limited company.
Personal Identification Secure Comparison and Evaluation System (PISCES)	This information allows CBP officers to access biographic and biometric information of travelers whose information was collected by DOS at an international airport. PISCES is owned by the DOS.
Terrorist Screening Database (TSDB)	CBP officers use this information to identify potential terrorists that need additional screening. TSDB information is part of an FBI system.



## Appendix B

### Forms Created In Unified Secondary

Unified Secondary maintains a copy of the data elements from the forms, but most forms will be recorded in EID as the system of record.

Form Name	OMB Number, if Applicable <sup>49</sup>
CBP-93 - Unaccompanied Alien Child Screening Addendum	
CBP-2500 - Alien Initial Health Interview Questionnaire	
TEDS - Detainee Assessment for Transport, Escort and Detention	
FD-936 - Request for National DNA Database Entry	
G-166F - Report of Investigation	
I-160 - Notice of Parole/Lookout Intercept	
I-160A - Notice of Refusal of Admission/Parole into the US	
I-193 - Application for Waiver of Passport and/or Visa	1651-0107
I-200 - Warrant of Arrest of Alien	
I-203 - Order to Detain or Release Alien	
I-205 - Warrant of Removal Removal/Deportation	
I-210 - Notice of Action - Voluntary Departure	
I-213 - Record of Deportable/Excludable Alien	
I-214 - Warning as to Rights - Interview Log	1651-0029
I-215B - Record of Sworn Statement in Affidavit Form	
I-216 - Record of Person and Property Transfer	1651-0029
I-217 - Information for Travel Document or Passport	
I-220A - Order of Release on Recognizance	
I-247A - Immigration Detainer - Notice of Action	
I-259 - Notice to Detain, Remove, or Present Alien	
I-263A - Record of Sworn Statement	
I-264 - Notice to Consular Officer Concerning Detention	
I-265 – Notice to Appear (NTA), Bond, and Custody Processing Sheet	

<sup>49</sup> Forms without OMB numbers are forms completed or issued by CBP that are not completed by the public and exempt from the PRA.



I-275 - Notice of Visa Cancellation/Border Crossing Card Voidance	
I-286 - Notice of Custody Determination	
I-294 - Warning of Removal/Deportation	
I-296 - Notice to Alien Ordered Removed/Departure Verification	
I-385 - Alien Booking Record	
I-407 - Abandonment of Lawful Permanent Resident Status	1615-0130
I-515A - Notice to Student and Exchange Visitor	1615-0083
I-546 - Order to Appear Deferred Inspection	
I-770 - Notice of Rights and Request for Disposition	
I-826 - Notice of Rights and Request for Disposition	
I-830 - Notice to EOIR: Alien Address	
I-844 - Notice of Intent to Deport for Violating the Terms of Your Admission Under Section 217 of the Immigration And Nationality Act	
I-848 - Notice of Rights and Request for Disposition for El Salvadorans	
I-848A - Notice of Rights and Request for Disposition for El Salvadorans	
I-849 - Record for Notice of Intent to Fine	
I-851 - Notice of Intent to Issue a Final Administrative Removal Order	
I-851A - Final Administrative Removal Order in Removal Proceedings Under Section 238(b) of the Immigration and Nationality Act	
I-860 - Notice and Order of Expedited Removal	
I-862 - Notice to Appear	
I-863 - Notice of Referral to Immigration Judge	
I-867A - Record of Sworn Statement in Proceedings under Section 235(b)(1) of the Act	
I-867B - Jurat for Record of Sworn Statement in Proceedings under Section 235(b)(1) of the Act	
I-871 - Notice of Intent / Decision to Re-Instate a Prior Order	
I-877 - Record of Sworn Statement in Administrative Proceedings	
I-99 - Notice of Revocation and Penalty	
M-444 - Information about Credible Fear Interview	
R-84 - Final Disposition Report (Goes to FBI)	1110-0051
Single Journey Letter to the Point of Embarkation	



Declination of Notification for Detention/Delay Pending a Determination of Admissibility	
Contact Advisory of CBP Detention	
Discretionary Authority Checklist for Alien Applicants (Discretionary Checklist)	
CDC Public Health Traveler Health Declaration Form	