Privacy Impact Assessment

for the

CBP Support of CDC for Public Health Contact Tracing

DHS Reference No. DHS/CBP/PIA-066

December 15, 2020

Homeland Security

Abstract

U.S. Customs and Border Protection (CBP) assists the Department of Health and Human Services (HHS), Centers for Disease Control and Prevention (CDC) with its public health response efforts. CBP has historically transmitted certain biographic information from travelers traveling to the United States from foreign locations to CDC, upon CDC's request, in support of CDC's efforts to contact individuals who may have been exposed to communicable diseases during their travels. CBP's support of CDC's public health response efforts has expanded since the COVID-19 pandemic. CBP is publishing this Privacy Impact Assessment (PIA) to discuss CBP's efforts to assist CDC by providing public health emergency response-related personally identifiable information (PII) to CDC.

Overview

CBP is charged with ensuring compliance with federal laws at the border, including those preventing contraband, other illegal goods, and inadmissible persons from entering the United States. CBP's border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to ensure compliance with any law or regulation enforced or administered by CBP, and to determine if the merchandise is subject to duty or being introduced into the United States contrary to law. CBP's mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies. CBP's duties include aiding the Department of Health and Human Services (HHS) Centers for Disease Control and Prevention (CDC) in the "enforcement of quarantine rules and regulations."[1]

HHS is the U.S. Government's principal agency for protecting the health and well-being of all individuals in the United States and has the statutory responsibility to make and enforce regulations necessary to prevent the introduction, transmission, or spread of communicable diseases from foreign countries into the United States and/or between U.S. states and territories.[2] The CDC, a component of HHS, has the statutory authority to detain, isolate, quarantine, or conditionally release persons arriving into the United States or those traveling between U.S. states or territories who are reasonably believed to be infected with quarantinable diseases.[3] Some of the activities the CDC undertakes to meet its statutory and regulatory responsibilities include overseeing screening of arriving international travelers for symptoms of illness that could constitute a quarantinable or other serious communicable disease, providing travelers with

[1] *See* 42 U.S.C. § 268.
[2] *See* 42 U.S.C. §§ 264-272.
[3] *Id.*

essential public health information, and implementing federal quarantine regulations.[4]

CDC Contact Tracing Efforts

According to the CDC, a fundamental component of a public health response is identifying and contacting travelers who may have come into contact with a person with a communicable disease and who may be at risk of contracting the disease as a result of their interactions with such affected persons. There is a significant public benefit from health authorities identifying, locating, and notifying exposed and potentially exposed travelers. In turn, this helps prevent the propagation and further spread of disease.

Based on CDC experience, the following data elements are critical to conduct effective contact tracing: (1) full name; (2) address while in the United States; (3) email address; (4) primary phone number; and (5) secondary/emergency contact phone number.

CBP's historical support of CDC Contact Tracing and expanded support in response to the 2020 COVID-19 Pandemic:

In support of CDC's efforts to manage and contain the spread of communicable diseases, CBP provides biographic information to CDC, when requested by CDC, regarding travelers who have traveled to the United States and are believed to have been exposed to a communicable disease during their international travel. CBP has historically assisted CDC in identifying persons who may have been exposed to an infectious disease while in international travel to the United States, and has provided CDC with contact information for such individuals upon request. CDC provided this information to state and local public health authorities so that they would be able to notify the individuals about their potential exposure and provide guidance to protect their health and that of the community. Under this historical process, the CDC would submit a request to CBP via the Homeland Security Information Network (HSIN).[5] Upon receiving a request, CBP personnel searched CBP holdings to identify travelers who may have come in contact with the infected traveler per the parameters provided by CDC. CBP pulled the relevant contact information related to travelers who may have come into contact with the infected traveler or otherwise requested by CDC and provided the available contact information back to CDC via HSIN.

On March 13, 2020, the White House declared a national emergency in the United States

[4] *See* 42 C.F.R. Chapter I, Subchapter F, Part 71, Foreign Quarantine.
[5] HSIN is the Department's official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international and private sector partners. Mission operators use HSIN to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE HSIN 3.0 SHARED SPACES ON THE SENSITIVE BUT UNCLASSIFIED NETWORK, DHS/ALL/PIA-061 (2012), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

concerning the COVID-19 Outbreak.[6] COVID-19 is a quarantinable disease as it falls within the scope of "severe acute respiratory syndromes," which are designated as quarantinable pursuant to Executive Order 13674.[7] One of the primary ways the CDC can stop the spread of diseases such as COVID-19 is through contact tracing and other public health follow-up activities.[8]

Section 212(f) of the Immigration & Nationality Act (INA) gives the President of the United States the authority to issue Presidential Proclamations to suspend entry of any alien travelers for a period of time deemed necessary by the President. On January 31, 2020, the White House issued the "Proclamation on Suspension of Entry as Immigrants and Nonimmigrants of Persons who Pose a Risk of Transmitting 2019 Novel Coronavirus,"[9] the first of several proclamations issued regarding COVID-19 related travel restrictions. These proclamations collectively suspended the entry of most aliens who, within the prior 14 days, had been in mainland China, Iran, the European Schengen Area, Ireland, the United Kingdom (excluding overseas territories outside of Europe), or Brazil.

As described above, CBP historically relied on CDC to submit requests to obtain contact information on certain travelers who may have been exposed to a disease during travel. Due to the COVID-19 pandemic, CBP has shifted the way it will now provide support to CDC. Following the series of Presidential Proclamations, CBP built automated rules within the Automated Targeting System (ATS)[10] to assist in enforcing these international travel restrictions as well as to identify non-restricted travelers who may have traveled to areas affected by an outbreak. CBP uses ATS to identify travelers who are permitted to travel to the United States and who have had recent travel to areas affected by the outbreak. CBP provides CDC with the contact information on travelers arriving in the United States with a nexus within the 14 days prior to arrival to 212(f) restricted countries. CBP sources this critical biographic information from a combination of CBP and non-CBP sources to support efforts to manage and contain the spread of quarantinable and serious communicable diseases, such as COVID-19. CBP provides information from the following datasets to CDC:

---

[6] *See* WHITE HOUSE, PROCLAMATION ON DECLARING A NATIONAL EMERGENCY CONCERNING THE NOVEL CORONAVIRUS DISEASE (COVID-19) OUTBREAK, (March 13, 2020), *available at* https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/.

[7] Exec. Order No. 13674, *Revised List of Quarantinable Communicable Diseases*, 79 Fed. Reg. 45671 (July 31, 2014).

[8] Contact tracing is the identification, monitoring, and support of the individuals who have been exposed to a communicable disease and have possibly become infected themselves.

[9] *See* https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-immigrants-nonimmigrants-persons-pose-risk-transmitting-2019-novel-coronavirus/.

[10] ATS is a decision support tool that aggregates data from various systems to compare traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. *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.

***CBP datasets*:**

- **Advance Passenger Information System (APIS):**[11] In accordance with CBP regulations, air carriers are required to send passenger and crew manifests to CBP before an air carrier departs from the foreign port or place for the United States.[12] The information within the manifest consists of biographic data elements such as name, U.S. address, date of birth, gender, country of citizenship, and travel document information. APIS is an electronic data interchange system used by DHS for collection of passenger and crew manifest data mandated by CBP regulations.
- **Global Enrollment System (GES):**[13] Global Enrollment System pre-approves travelers arriving in the United States for expedited processing at designated U.S. Ports of Entry (POE) or for access to sensitive CBP-controlled areas or positions.
- **Electronic System for Travel Authorization (ESTA):**[14] The Visa Waiver Program (VWP) permits travelers from certain countries to come to the United States without first obtaining a visa. Participation in the VWP requires enrollment in CBP's ESTA program.
- **Electronic Visa Update System (EVUS):**[15] CBP's EVUS is a web-based enrollment system used to collect information from nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program, and 2) have been issued a U.S. nonimmigrant visa of a designated category. EVUS, similar to ESTA, collects updated information in advance of an individual's travel to the United States.
- **Passenger Name Record (PNR) data:**[16] 49 U.S.C. § 44909(c)(3) and its

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM, DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[12] 19 C.F.R. §§ 122.49a, 122.49b.
[13] *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.
[14] *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.
[15] *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.
[16] This information is collected from air carrier travel reservations and is transmitted to CBP prior to the flight's departure. PNR data provided to CBP may differ depending on the particular air carrier collecting the data since air carriers do not all collect the same set of information. The PNR data collected by air carriers and submitted to CBP generally includes the traveler's name, contact details, details of the travel itinerary (such as date of travel, origin and destination, seat number, and number of bags) and details of the reservation (such as travel agency and payment information). CBP stores PNR data in ATS.

implementing regulation at 19 C.F.R. § 122.49d require air carriers operating flights to or from the United States to provide CBP with certain passenger reservation information, called PNR data, to the extent it is collected and contained in the air carrier's reservation and/or departure control systems. Such data is primarily used by CBP to prevent, detect, investigate, and prosecute terrorist offenses and related crimes and certain other crimes that are transnational in nature.

- **Voluntary submissions from air carriers or other travel providers:** As described above, air carriers are required to send CBP passenger and crew manifest information to CBP APIS. These regulations only require air carriers to provide a specified list of data elements, including each passenger's name and U.S. address (address information is not required for U.S. citizens, lawful permanent residents (LPR), or persons who are in transit). However, in addition to the mandatory data elements, air carriers may voluntarily choose to submit additional non-required information to CBP via their APIS transmissions, including passengers' phone numbers, secondary/emergency contact numbers, and email addresses. Air carriers may also choose to transmit additional data through PNR transmissions. For example, air carriers may already, as part of their routine business practices, collect contact information as part of the passenger reservation information or PNR data.[17] Air carriers that use PNR data may choose to begin sending the additional contact information through their existing PNR feed to ATS. Alternatively, air carriers may submit these elements to CBP directly through a JavaScript Object Notation (JSON)[18] connection that is correlated by CBP with APIS.

  CBP already collects or has access to these data elements voluntarily submitted through air carriers for a vast majority of travelers through various means. However, this biographic information is often incomplete for some travelers, especially U.S. citizens and LPRs, who are not required to provide a U.S. address in APIS.

***Non-CBP Datasets*:**

- **U.S. Citizenship and Immigration Services (USCIS):** USCIS oversees lawful immigration to the United States and is responsible for processing immigration requests, including granting lawful permanent residence and granting citizenship. In order to effectively grant or deny an immigration request, USCIS collects and

[17] CBP currently collects PNR information from air carriers, as authorized by 49 U.S.C. § 44909(c)(3) and the implementing regulation at 19 C.F.R. § 122.49d. These statutory and regulatory authorities require each air carrier operating passenger flights in foreign air transportation to or from the United States to provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.
[18] JSON is type of data format.

maintains a large amount of PII from immigration requestors, including the individual's contact information. To support CDC's public health follow-up efforts, CDC requested that USCIS supply CDC with biographic information on both LPRs and LPRs with pending/approved N-400, *Application for Naturalizations*, using CBP's existing architecture with both USCIS and the CDC. This information is originally sourced from USCIS systems including Computer Linked Application Information Management System 3 (CLAIMS 3),[19] USCIS Electronic Immigration System (USCIS) ELIS,[20] and Central Index System (CIS 2).[21] CBP plans to begin sharing this information with CDC in early 2021.

- **Department of State (DOS) nonimmigrant visa and immigrant visa application data:**[22] A citizen of a foreign country who seeks to enter the United States generally must first obtain a U.S. visa, which is placed in the traveler's passport, a travel document issued by the traveler's country of citizenship. Travelers who are seeking to travel to the United States on a temporary basis may obtain a nonimmigrant visa, while travelers who are intending to live permanently in the United States may obtain an immigrant visa. Historically, DOS has shared certain nonimmigrant and immigrant visa application data from certain posts with CBP. In response to the 2020 COVID-19 pandemic, DOS agreed to expand its sharing to include all worldwide visa applications with CBP to perform vetting. DOS has agreed to allow CBP to share this information with CDC.

This information is shared with CDC pursuant to a 2005 Memorandum of Understanding (MOU) between HHS and DHS,[23] routine uses in the applicable SORNs,[24] and letters and policy memorandums between CBP and internal and external partners.

---

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016 (2008 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

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

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

[22] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (2015), *available at* https://www.state.gov/documents/organization/242316.pdf. Certain international travelers may be eligible to travel to the United States without a visa if they meet the requirements for visa-free travel.

[23] Memorandum of Understanding, *The Department of Health and Human Services and The Department of Homeland Security* (October 19, 2005).

[24] CBP also shares this information with CDC pursuant to various routine uses in applicable DHS SORNs. The routine use permits CBP to share this information with CDC "…to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combating other significant public health threats…" *See*, for example, DHS/CBP-006 Automated Targeting System, *supra* note 25.

Aggregation and Transmission of Data to CDC

Due to the massive level of contact tracing and other public health follow-up activities required in response to the 2020 COVID-19 pandemic, in addition to the ATS rules, CBP developed an automated method to share the information with CDC. Using ATS, CBP extracts all available contact information and relevant travel information on travelers whose data is to be provided to CDC from the datasets described above. By extracting this data, ATS builds a person-centric record regarding each traveler. The person-centric record consists of the following information, when available in the source system:

- Traveler Name;
- Date of Birth;
- Travel Document (APIS includes document type, number, and country of issuance);
- Citizenship;
- Gender (sourced from APIS);
- Mode of Entry;
    - For Air and Sea: Flight or Vessel information, including arrival port and arrival date (sourced from APIS);
    - For Land: Conveyance information, when available, including the arrival port and arrival date (sourced from the Primary to Secondary referral);
- U.S. Address (sourced from GES/ESTA/EVUS/DOS Visa/APIS/PNR/USCIS data);
- Primary and Secondary contact phone numbers (sourced from GES/ESTA/EVUS/DOS Visa/PNR/USCIS data); and
- Email address (sourced from GES/ESTA/EVUS/DOS Visa/PNR/USCIS data).

CBP will provide these records to the CDC within eight hours of the traveler's arrival into the United States, or as otherwise requested by CDC.

CBP will send any and all available contact information from the above listed sources to the CDC. Therefore, CBP may provide the CDC with multiple entries for each data field. For example, if CBP has a different phone number from a traveler's PNR and visa application, CBP will provide CDC with both phone numbers. This vastly increases the chance of successfully contacting a traveler and ultimately assists the CDC in reducing the spread of communicable diseases, such as COVID-19.

CDC Division of Global Migration and Quarantine (DGMQ) Quarantine Public Health Officers will use this contact information to notify state and local public health entities to contact

travelers who may have been exposed to a communicable disease during travel and identify appropriate public health interventions. In general, state and local public health entities are responsible for this public health follow-up. In rare cases, CDC may use the data to perform the contact investigation directly. In either case, CDC works with state and local public health entities so that travelers can receive appropriate public health follow-up.

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?

CDC has the authority to collect this information under the Public Health Service Act (42 U.S.C. § 264), 42 C.F.R. §§ 71.4 and 71.20, and 85 Fed. Reg. 7874 (Feb. 12, 2020). CBP has the authority to assist CDC under 42 U.S.C. § 268(b), which states that it "shall be the duty of the customs officers . . . to aid in the enforcement of quarantine rules and regulations." CBP will also use the data in accordance with the authorities that govern ATS. ATS derives its authority from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

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

CBP maintains this information in ATS in accordance with the DHS/CBP-006 Automated Targeting System SORN.[25] Per the published SORN, CBP uses ATS to retain information about persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea. One of ATS's purposes is to otherwise assist in the enforcement of the laws enforced or administered by DHS, which necessarily includes 42 U.S.C. § 268(b), which states that it "shall be the duty of the customs officers . . . to aid in the enforcement of quarantine rules and regulations."

CBP provides information to CDC from various sources though and are covered by the following SORNs:

[25] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

- **APIS:** APIS SORN[26]
- **GES:** Trusted and Registered Traveler Programs SORN[27]
- **ESTA:** ESTA SORN[28]
- **EVUS:** EVUS SORN[29]
- **PNR:** ATS SORN
- **Voluntary Air Submissions:** ATS and APIS SORNs
- **USCIS Data:** Benefits Information System[30] and Alien File[31] SORNs
- **DOS Visa Data**: Consular Consolidated Database SORN[32]

CDC maintains the records provided by CBP in accordance with its system of records notice, SORN No. 09-20-0171.[33]

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

Yes. All CBP source systems have undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. ATS, as the system responsive for creating an aggregated record, received a renewed Authority to Operate on January 26, 2020.

---

[26] *See* DHS/CBP/PIA-001 Advance Passenger Information System, 80 Fed. Reg. 13407 (March 13, 2005), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[27] *See* DHS/CBP-002 Trusted and Registered Traveler Programs, 85 Fed. Reg. 14214 (March 11, 2020) *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[28] *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 84 Fed. Reg. 30746 (June 27, 2019), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[29] *See* DHS/CBP-022 Electronic Visa Update System (EVUS), 84 Fed. Reg. 30751 (June 27, 2019), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[30] *See* DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.
[31] *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-notices-sorns.
[32] *See* STATE-39 Visa Records, 83 Fed. Reg. 28062 (June 15, 2018), *available at* https://www.federalregister.gov/documents/2018/06/15/2018-12871/privacy-act-of-1974-system-of-records.
[33] *See* SORN 09-20-0171, Quarantine- and Traveler-Related Activities, Including Records for Contact Tracing Investigation and Notification under 42 C.F.R. Parts 70 and 71, 72 Fed. Reg. 70867 (December 13, 2007), *available at* https://www.federalregister.gov/documents/2007/12/13/E7-24142/privacy-act-of-1974-new-system-of-records, and as amended by 76 Fed. Reg. 4485 (January 25, 2011), *available at* https://www.federalregister.gov/documents/2011/01/25/2010-33029/privacy-act-of-1974-report-of-modified-or-altered-system-of-records, and as amended by 83 Fed. Reg. 6591 (February 14, 2018), *available at* https://www.federalregister.gov/documents/2018/02/14/2018-03014/privacy-act-of-1974-system-of-records.

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

Each source has its own retention period. ATS consolidates and stores all available contact information for a period of 15 years. Contact tracing records will be maintained by CDC until the contact investigation is complete or no longer than 12 months, in accordance with proposed retention schedules as designated by CDC's SORN(s).

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.

CBP is relying on several sources of information to supply data to the CDC. Many of the sources of information collect information directly from the individual (e.g., ESTA, EVUS, or visa application) and may be subject to the PRA.

Section 2.0 Characterization of the Information

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

ATS aggregates various types of data from various systems and datasets (e.g., APIS, GES, ESTA, EVUS, PNR, and DOS visa information). With the aggregated data, ATS: (1) performs targeting of individuals who may pose a risk to border security or public safety, may be identified as a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law; (2) performs risk-based assessments of conveyances and cargo to focus CBP's resources for inspection and examination and to enhance CBP's ability to identify potential violations of U.S. law, possible terrorist threats, and other threats to border security; and (3) otherwise assists in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism. CBP does not routinely share amalgamated records from ATS with other agencies; however, for contact tracing purposes, CBP is creating and sharing this type of record from ATS with CDC.

CBP shares the following information with CDC from CBP's holdings:

- Traveler Name;
- Date of Birth;
- Travel Document (e.g., passport number and country of issuance);

- Citizenship;
- Gender;
- Mode of Entry;
- Flight Information;
- Conveyance information, including the arrival port and arrival date;
- U.S. Address;
- Primary Contact Phone Number;
- Secondary and/or Emergency Contact Numbers; and
- Email Address.

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

Pursuant to 42 U.S.C. § 268(b), CBP will assist in collecting and transmitting accurate and up-to-date contact information to CDC from CBP holdings. The information from CBP holdings may be found in ATS but is originally derived from CBP and non-CBP sources. The sources CBP provides include: APIS, GES, ESTA, EVUS, PNR, voluntary air submissions, USCIS LPR and Naturalization Data, and DOS Visa data. In many cases, the original source system collects information directly from the individual (e.g., DOS visa applications are completed by the applicant).

Additionally, CBP may transmit information originally supplied through the travelers or through a travel agent as part of the booking/check-in process. Air carriers may transmit this information to CBP through a pre-existing connection, such as the APIS feed, PNR feed, or JSON interface.

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

No.

2.4 Discuss how accuracy of the data is ensured.

Although the contact information on travelers may be supplied in various ways, the original point of collection is from the airline carrier (at booking/check-in, for example), or by way of a U.S. Government collection that is typically collected originally from the individual (e.g., ESTA, EVUS, or visa application). In all scenarios, CDC and CBP assume the information to be accurate

and complete, since the information is typically originally supplied directly from the individual to whom the collection of information pertains.

CBP provides a consolidated list of all available contact information to CDC regarding travelers arriving to the United States with a nexus within the 14 days prior to arrival to 212(f) restricted countries. Therefore, CBP may provide CDC with multiple entries for each data field. For example, if CBP has multiple phone numbers from a trusted traveler application and ESTA application, CBP will provide CDC with both phone numbers. This vastly increases the chance of successfully contacting a traveler and ultimately assists CDC in reducing the spread of communicable diseases, such as COVID-19.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that CBP will provide CDC inaccurate information from its holdings or create a mismatch during the amalgamation process.

Mitigation: This risk is partially mitigated. As described above, CBP will supply CDC with person-centric records that are created using a combination of the information from various sources. Depending on when the information was ingested into CBP holdings, or when the information was collected by the air carrier (e.g., upon booking versus right before departure), it is possible the information may no longer be accurate. CBP is providing a person-centric travel record to CDC that may contain multiple pieces of contact information (e.g., multiple phone numbers or email addresses) to increase the chances of public health officials successfully contacting a traveler. CBP provides CDC with the source of the data, as well as the date associated with the source record, so to inform CDC of the recency of the information.

Although old or outdated information may be provided to CDC, the goal of the sharing is to provide CDC with adequate contact information for CDC to fulfill its public health responsibilities related to contact tracing.

Privacy Risk: There is a risk that CBP is collecting and sharing too much information with CDC to perform public health follow-up activities.

Mitigation: This risk is mitigated. Based on CDC's experience, in order to conduct effective contact tracing of travelers who arrive in the United States from abroad, it is critical to have the person's full name, address in the United States, one or two phone numbers, and email address. In the past, CDC has reviewed the effectiveness of different means of contacting a person.[34] If public health authorities have a valid phone number, the contact rate is between 91 and 100 percent. With only the address, the contact rate drops to 44 percent. With only the name—currently, a common situation—the contact rate is only eight percent. HHS and CDC have found

[34] 85 Fed. Reg. 7874 (February 12, 2020).

that a phone number will allow rapid contact with a traveler and can substantially improve the public health response to an outbreak. Two phone numbers increase the chance of contacting a traveler, even when he or she is traveling. HHS and CDC believe that collecting email addresses will further increase the chance of contacting a person when he or she is traveling. Moreover, especially in an outbreak where CDC and its public health partners will need to conduct a significant amount of contact tracing as quickly as possible, it is critical for CDC to receive the information in a usable electronic form, so that it is easy to process, analyze, and, as necessary, transmit to its public health partners.

Privacy Risk: There is a risk that CBP will begin receiving and using information from U.S. citizens and LPRs that CBP did not previously require or collect on a consistent basis.

Mitigation: This risk is partially mitigated. Pursuant to the ATS SORN, CBP has the authority to collect and receive biographic data elements, such as address and phone number, from U.S. citizens and LPRs to perform a risk-based assessment of travelers, conveyances, and cargo to focus CBP's resources for inspection and examination and enhance CBP's ability to identify potential violations of U.S. law, possible terrorist threats, and other threats to border security; and to otherwise assist in the enforcement of the laws enforced or administered by DHS.

As with any other biographic information collected by CBP and stored within ATS, CBP uses this information for vetting and targeting purposes to identify individuals who may need additional scrutiny. The limited amount of expanded contact information CBP will receive as part of this effort is consistent with CBP border security authorities and will be used to perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. With the emergent nature of public health emergencies, and to mitigate any undue privacy risks as these emergencies develop and change in nature, CBP will continue to analyze and determine whether the information collected and further shared is appropriate

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Pursuant to 42 U.S.C. § 268(b), CBP will assist in collecting and transmitting contact information to CDC from CBP holdings to support CDC's contact tracing efforts. CBP derives the information from various internal and external sources accessible in ATS. One of ATS's purposes is to otherwise assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism. This necessarily includes 42 U.S.C. § 268(b), which states that it "shall be the duty of the customs officers . . . to aid in the enforcement of quarantine rules and regulations." These data elements are aggregated in ATS to generate person-centric traveler records, which may be used by system users with the authority to access the relevant underlying datasets based on the authorized user's official responsibilities, including to facilitate CBP traveler

screening and vetting, law enforcement, border security, public security, counterterrorism, and national security missions, as appropriate.

CBP will transfer the person-centric records to CDC within eight hours of a traveler's arrival in the United States to assist in CDC's contact tracing responsibilities. In turn, CDC will provide the contact information for exposed travelers to state and local health authorities to perform contact tracing, as appropriate. These entities will use the contact information to locate travelers and inform them about their exposure and what to do (e.g., what symptoms to look out for, how to get tested, recommendation to quarantine).

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.

Yes. ATS is used to compare existing information about travelers and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.

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

CBP is not routinely sharing the amalgamated information with any entity other than CDC. However, DHS components who have access to ATS may access the APIS, GES, ESTA, EVUS, PNR, voluntary air submissions, USCIS LPR and Naturalization Data, and DOS Visa data on a need to know basis consistent with the component's mission pursuant to 5 U.S.C. § 552a(b)(1) (the Privacy Act). The following DHS components currently have access to ATS:

- U.S. Immigration and Customs Enforcement (ICE);
- U.S. Citizenship and Immigration Services (USCIS);
- DHS Office of Inspector General (OIG);
- DHS Office of Intelligence & Analysis (I&A);
- United States Coast Guard (USCG); and
- Transportation Security Administration (TSA).

Access to ATS is role-based and assigned according to the mission of the component and the user's need to know. Furthermore, access to specific datasets within ATS is further controlled by providing each user only those accesses required to perform his or her job.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP will use expanded biographic information from voluntary air carrier submissions beyond the purpose of contact tracing.

Mitigation: This risk is not mitigated. Air carriers may voluntarily submit this expanded biographic contact information to CBP. As with any other biographic information collected by CBP and stored within ATS, CBP uses this information for vetting and targeting purposes to identify individuals who may need additional scrutiny. The limited amount of expanded contact information that air carriers voluntarily provide to CBP is consistent with CBP border security authorities and will be shared with CDC to conduct contact tracing and also used by CBP to perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.

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.

This PIA provides notice of this data collection and use for contact tracing purposes. The source system PIAs outlined above provide general notice for the collection of information Furthermore, the CDC and ATS SORNs also include routine uses that describe what external disclosures are permitted to share this information. Furthermore, additional measures may be taken by agencies or private entities (e.g., air carriers) to inform individuals of these efforts.

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

In most circumstances, ATS aggregates various types of data from various systems and datasets (e.g., APIS, GES, ESTA, EVUS, PNR, DOS visa, and USCIS LPR and naturalization data). At the original point of collection for these datasets, individuals are provided with a Privacy Act Statement, when feasible, notifying individuals with how their information may be used or shared with federal, state, and local government agencies, members of Congress, and officials of foreign governments in accordance with certain approved routine uses in the applicable SORNs. As described above, the respective SORNs include Routine Uses detailing how information may be shared with the CDC.

Privacy Act Statements are included on the applications/forms (e.g., ESTA, EVUS) that collect information that is then stored in the source systems listed above; individuals may opt out of providing certain information at that time. However, typically, individuals must provide certain

information when applying for an immigration benefit, visa, or trusted traveler program. If an individual opts out of or declines to provide certain information, he or she may become ineligible to receive the immigration benefit, visa, or program benefit being applied for (e.g., preventing the individual from participating in a trusted traveler program or from receiving a visa). Further, when booking or checking-in for air travel, for example, it is the responsibility of the air carrier to provide notice to the individual on the provision of information to CBP and CDC (e.g., APIS and PNR data). Under these circumstances, if the individual does not consent to supplying information to the air carrier, which then provides information to CBP/CDC, he or she may be unable to complete travel. However, as part of voluntary air carrier submissions, the air carriers may request that travelers voluntarily provide an expanded set of data elements (e.g., email, secondary/emergency contact phone number). If a traveler opts in to providing the additional contact information, the air carriers submit this information to CBP, which then provides the information to CDC.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the public does not have sufficient notice of CBP sharing information with CDC for the purpose of contact tracing.

Mitigation: This risk is partially mitigated. This PIA provides notice to the public on CBP sharing information with CDC to assist CDC with their public health responsibilities. CBP is issuing this comprehensive PIA to discuss this sharing and the risks and mitigations associated with it. The CDC has also published extensive information on the CDC website to discuss the importance and benefits of contact tracing. While the concept of contact tracing has recently become well-known, the CDC in conjunction with state and local public health authorities has been conducting contact tracing for years for other illnesses such as Tuberculosis and Ebola.

Privacy Risk: There is a risk that travelers cannot decline participation or opt out of participating with this information collection.

Mitigation: This risk is partially mitigated. Depending on the method of collection (e.g., voluntary air carrier submissions), travelers may have the opportunity to opt out of providing this information to CBP, which would then share the information with CDC, when the collection or provision of the information is voluntary. However, CBP is largely providing CDC with information already within CBP holdings, where travelers will not have the opportunity to explicitly opt out of providing information. This information is necessary to identify, monitor, and support travelers who have been exposed to, and possibly infected with a communicable disease such as COVID-19. Prompt identification, voluntary quarantine, and monitoring of exposed individuals can effectively break the chain of disease transmission and prevent further spread in a community. If the individual does not consent to supplying information to an air carrier, he or she may simply be unable to complete his or her travel.

Privacy Risk: There is a risk that travelers (and their secondary/emergency contacts) are not aware that the information they are supplying to the air carriers will be collected and used by the U.S. Government for public health emergency contact tracing.

Mitigation: This risk is partially mitigated. Air carriers have a long-standing commitment to supply CBP with manifest data, as required by federal law, including CBP's APIS regulations. In response to the COVID-19 pandemic, air carriers may choose to submit additional data to CBP, beyond what is required in the APIS regulations. When booking or checking-in for travel, it is possible the traveler is not aware that his or her information will be supplied to the U.S. Government for contact tracing and DHS mission related purposes. However, CDC and CBP places the onus on the travel providers (e.g., air carriers) to supply notice to the traveler. This PIA also provides a measure of notice.

Further, passengers regularly provide CBP with contact information for non-travelers to serve as a point of contact for them while the traveler is in the United States (e.g., ESTA). This PIA and the notice provided by travel providers informs them of this collection.

Section 5.0 Data Retention by the Project

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

CBP retains the data in ATS for 15 years.[35] Contact tracing records will be maintained by CDC until the contact investigation is complete or for no longer than 12 months, in accordance with proposed retention schedules and CDC's SORN(s).

5.1 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CBP is retaining the contact information for longer than necessary.

Mitigation: This risk is partially mitigated. The justification for a 15-year retention period for the official records is based on CBP's law enforcement and security functions at the border. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP officers with their risk-based assessment of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

[35] *See* DHS/CBP-006 Automated Targeting System, *supra* note 25.

If the record is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, travelers, and routes of concern; or other defined sets of circumstances), the record will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related, which are retained for 75 years, in accordance with the TECS SORN.[36]

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.

CBP has been routinely providing information to CDC in support of the CDC's mission for over a decade pursuant to a 2005 DHS-HHS MOU and routine uses in the relevant SORNs. Upon receipt from CBP, CDC shares the information with state and local public health departments so they can contact travelers who may have been exposed to a communicable disease during travel and identify appropriate public health interventions. In general, state and local public health departments are responsible for this public health follow-up. In rare cases, CDC may use the data to perform the contact investigation directly. In either case, CDC works with state and local health departments so that travelers can receive appropriate public health follow-up.

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

CBP shares this information with CDC pursuant to Routine Use J of the ATS SORN. Routine Use J permits CBP to share information: "To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk." The sharing to CDC is consistent and compatible with the purpose of CBP's original collection of the information, which supports CBP's enforcement of numerous federal laws at the border, and consistent with the broader CBP mission of safeguarding the nation while facilitating legitimate trade and travel.

[36] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

6.3 Does the project place limitations on re-dissemination?

CBP permits CDC to re-disseminate this information to state and local domestic public health departments for public health follow-up. As described in the 2005 MOU, CDC may not further disseminate without prior consent from CBP.

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

CBP maintains an audit log within ATS to record the exchange of information with CDC.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CBP will share the amalgamated data under inappropriate circumstances, or with entities without a demonstrated need to know.

Mitigation: This risk is mitigated. Risks related to ongoing sharing of information outside DHS, including any potential risk of further dissemination of information by the external agency to a third agency, are mitigated through arrangements governing access to information in ATS by external parties. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being accessed or shared and the legal basis upon which they receive it. The arrangements generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by DHS. Lastly, CBP emphasizes that within each arrangement, each external user is provided with training designed to ensure that data accessed through ATS is safeguarded and secured in an appropriate manner and that dissemination restrictions are observed, consistent with applicable laws and policies.

Privacy Risk: There is a risk that CBP is oversharing information with CDC.

Mitigation: This risk is partially mitigated. Previously, CDC requested and received records from CBP on an ad hoc basis. This included a limited subset of information based on what was available in CBP holdings. With the publication of this PIA, CBP is documenting the increased support CBP is providing to CDC in response to the 2020 COVID-19 pandemic. As requested by CDC, CBP is now sending contact information to CDC on individuals arriving in the United States who have a nexus to a 212(f) restricted country. This information includes expanded information sharing on U.S. citizens and LPRs (via the voluntary air carrier submissions), as well as a larger set of visa applicants to help prevent the further transmission and infection of communicable diseases, such as COVID-19.

CBP, USCIS, and DOS include Routine Uses in their applicable SORNs that permit the sharing of this information with CDC in support of CDC's public health responsibilities. Routine Use A of the STATE-39 SORN, which covers the collection of visa applications, permits DOS to share information with DHS "for uses within its statutory mission, including to process, approve,

or deny visa petitions and waivers, as well as for law enforcement, counterterrorism, transportation and border security, administration of immigrant benefits, critical infrastructure protection, fraud prevention, or employment verification purposes." Furthermore, Routine Use M permits DOS to share information with the CDC "for uses within its statutory mission."

Routine Use R of DHS/USCIS-007 Benefits Information System, which covers the collection of immigration requests, permits USCIS to share information "consistent with the requirements of the INA to the HHS, CDC, or to any state or local health authorities, … to ensure that all health issues potentially affecting public health and safety in the U.S. are being, or have been, adequately addressed." CBP SORNs include a Routine Use permitting CBP to share information "to appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk."

Section 7.0 Redress

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

To gain access to the information stored by CDC, a traveler may request information about his or her records through procedures provided by the Freedom of Information Act (FOIA)[37] and the access provisions of the Privacy Act of 1974.[38] CDC FOIA procedures are available at https://www.cdc.gov/od/foia/index.htm.

An individual may gain access to his or her CBP records by filing a Privacy Act (PA) or Freedom of Information (FOIA) request. Only U.S. citizens, LPRs, and individuals covered by the Judicial Redress Act of 2015 (JRA) may file a Privacy Act request. Any person, regardless of immigration status, may file a FOIA request.

Individuals are encouraged to make a FOIA request via FOIA Online at https://foiaonline.gov/foiaonline/action/public/home.

When seeking these records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. A traveler must provide his or her full name, current address, and date and place of birth. He or she must also provide:

[37] 5 U.S.C. § 552.
[38] 5 U.S.C. § 552a(d).

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when her or she believes the records would have been created;
- And if the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

Persons who have experienced difficulties while traveling may submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

TRIP is available for travelers to submit redress requests when experiencing difficulties traveling. Travelers may express concerns with supplying information to CDC via CBP for contact tracing via the CBP Information Center at www.help.cbp.gov.

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

Travelers wishing to correct inaccurate information may submit a Privacy Act amendment request through the same access processes explained above in Section 7.1. Additionally, individuals may be able to contact their travel providers to correct any information submitted to them, and the applicable SORNs provide travelers with notice of how to correct any inaccurate data.

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

This PIA and the applicable SORNs provide travelers with notice of how to correct any inaccurate data.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that a traveler may not have the opportunity to access or appropriately correct his or her information.

Mitigation: This risk is mitigated. CBP and CDC provide travelers with the opportunity to access or correct their information; either by submitting a FOIA or Privacy Act request, depending on the redress mechanism applicable to them. However, only CBP and CDC FOIA officers review FOIA and Privacy Act requests to determine if the requested information can be released or amended. The CDC SORN, "Quarantine and Traveler-Related Activities, Including Records for Contact Tracing Investigation and Notification under 42 C.F.R. Parts 70 and 71, HHS/CDC/CCID," does not claim any Privacy Act exemptions, meaning records are likely to be accessible to the traveler. The CBP ATS SORN does claim Privacy Act exemptions. Therefore, not all information covered by this SORN is available for redress. For example, records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information may not be accessible to the traveler.

Additionally, travelers can request correction of erroneous data stored in DHS databases through DHS TRIP.

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?

The CBP, USCIS, and DOS information is only available to users via ATS, which has role-based access. All user groups have access to the system as defined by their specific profile. Access is restricted based on roles and a demonstrated need to know. ATS secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS

Sensitive Systems Policy Directive 4300A.[39] This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. CBP periodically evaluates these systems to ensure that it complies with these security requirements.

Each system provides audit trail capabilities in order to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. CBP periodically conducts reviews for compliance within the program and between external partners to ensure that the information is used in accordance with the stated acceptable uses documented in the MOU, SORN, sharing agreements, and other technical and business documentation.

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

Initial ATS access is not activated for any user without completion of the CBP Security and Privacy Awareness course, which is required to be completed on an annual basis. This course presents Privacy Act responsibilities and agency policy regarding the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and ATS users are required to take the course annually.

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

Each user group's access to information in ATS is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common need to know and mission responsibilities of users within the group. Access by Users, Managers, System Administrators, Developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions. User access to data is based on a demonstrated need to know by a user, and access is only granted with supervisory approval and upon completion of the required security checks.

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

[39] *See* DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

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.

Responsible Official

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

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

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