Privacy Impact Assessment

for the

Advance Passenger Information System (APIS): Voluntary Expansion

DHS Reference No. DHS/CBP/PIA-001(i)

February 10, 2021

Homeland Security

Abstract

U.S. Customs and Border Protection (CBP) has collected mandatory and voluntary advance passenger information (API) from air, rail, bus, and sea carriers for over a decade. CBP uses API to identify high-risk passengers and crew members who may pose a risk to border, aviation, or public security; may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists; may be inadmissible; may be a person of interest; may otherwise be engaged in activity in violation of U.S. law; or may be the subject of wants or warrants. CBP is publishing this update to the longstanding Advance Passenger Information System (APIS) Privacy Impact Assessment (PIA) series to: 1) expand the collection and receipt of voluntary API in the air, land, and sea environments, including from bridge and ferry operators; 2) document the collection of expanded biographic information from carriers; and, 3) update the data retention period to 13 months.

Overview

CBP collects what is commonly referred to as API prior to a traveler's arrival at, departure from, or transit through the United States. The collection of API allows CBP to perform enforcement and security queries against various multi-agency law enforcement and terrorist databases and identify high-risk passengers and crew members who may pose a risk or threat to national security or public safety, or of non-compliance with U.S. civil and criminal laws, while simultaneously facilitating the travel of legitimate passengers and crew members. This information, often collected and maintained on what is referred to as the passenger manifest, is a combination of information found on travel documents (e.g., name, passport number, citizenship information) and carrier provided information (e.g., International Air Transport Association (IATA) codes, vessel names), including:

- Full name (last, first, and, if available, middle);
- Date of birth;
- Gender (F = female; M = male);
- Country of Citizenship;
- Country of residence;
- Status on board the conveyance;
- Travel document type (e.g., P = passport; A = alien registration card);
- Passport number, if a passport is required;
- Passport country of issuance, if a passport is required;

- Passport expiration date, if a passport is required for travel;
- Alien registration number (A-Number), where applicable;
- Address while in the United States (number and street, city, state, and zip code), except that this information is not required for U.S. citizens, lawful permanent residents (LPR), or persons who are in transit to a location outside the United States;
- Passenger Name Record (PNR) locator, if available;
- International Air Transport Association (IATA) code of foreign port/place where transportation to the United States began (foreign port code);
- IATA code of port/place of first arrival (arrival port code);
- IATA code of final foreign port/place of destination for in-transit passengers (foreign port code);
- Vessel name;
- Vessel country of registry/flag;
- Conveyance code and number (e.g., Airline carrier code, bus or rail carrier code/International Maritime Organization number, flight, bus, or train number);
- Date of arrival;
- Country/point of origin; and
- Final Destination.

In 2005, CBP issued a Final Rule[1] implementing the statutory mandates for air and sea carriers to submit API to CBP. Since then, CBP has also mandated the submission of API by pilots operating private aircraft[2] and has received voluntary API submissions from bus and rail carriers.

Mandatory API submissions

Current regulations[3] require that commercial air and vessel carriers and private aircraft pilots provide CBP with API about passengers and crew members traveling by air or sea and arriving in and/or departing from (and, in the case of aircraft crew, overflying) the United States.[4] Air and vessel carriers typically collect this information as part of the booking process and submit

[1] 70 Fed. Reg. 17820 (April 7, 2005).
[2] 73 Fed. Reg. 68295 (November 18, 2008).
[3] CBP's APIS regulations include 19 CFR 4.7b, 4.64, 122.22, 122.49a, 122.49b, 122.49c, 122.75a, and 122.75b.
[4] Public aircraft as defined under 19 CFR 122.1 (i) are exempt from providing API to DHS/CBP. U.S. military aircraft operating as public aircraft are exempt from providing API. However, when a military aircraft is transporting non-military personnel it is treated as a commercial airline and required to submit manifest information for the nonmilitary personnel.

the information to CBP using one of several submission methods. Commercial air carriers submit this information to CBP via the DHS Router, a messaging gateway between aircraft and cruise operators and the CBP Pre-Departure Service.[5] Private aircraft pilots, and certain commercial air carriers, submit information to CBP through the Electronic Advance Passenger Information System (eAPIS) web interface.[6] Commercial vessels submit passenger and crew manifest information through the U.S. Coast Guard's National Vessel Movement Center's Notice of Arrival and Departure System (NOAD).[7] All submission methods have a direct connection to the Advance Passenger Information System (APIS) for storage.

Voluntary API submissions

In addition to the mandatory air and sea submissions, CBP receives voluntary APIS submissions from rail and bus carriers.[8] To fulfill its border enforcement mission more efficiently, CBP needs to be able to accurately assess the threat risk of individuals entering the United States, including passengers and crew members aboard rail and bus traffic crossing the border.

Private and commercial rail and bus carriers may submit passenger and crew manifests to CBP via direct system connections or through the eAPIS web interface. This information is submitted into eAPIS from either the carrier or a third-party contractor hired on behalf of the carrier to gather and submit passenger and crew information. Passenger and crew information successfully submitted into the eAPIS web interface and received by CBP is stored as APIS data.[9]

---

[5] CBP Pre-Departure Service queries passenger names against Electronic System for Travel Authorization (ESTA), Electronic Visa Update System (EVUS), and TECS in order to verify passenger identity and ensure that individuals have the proper visas and other documents to enter the United States. The results of the checks are sent back to the DHS Router, which sends a "board"/"no board" message back to the operators for them to determine whether to allow the passenger to board.

[6] eAPIS is a CBP web-based computer application that provides for the collection of electronic traveler manifest information from commercial carriers and private aircraft pilots for international travel both into and out of the United States. The eAPIS website is *available at*: https://eapis.cbp.dhs.gov/.

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD, PRIVACY IMPACT ASSESSMENT FOR THE VESSEL REQUIREMENTS FOR NOTICES OF ARRIVAL AND DEPARTURE (NOAD) and AUTOMATIC IDENTIFICATION SYSTEM (AIS), DHS/USCG/PIA-006 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-coast-guard.

[8] Under 19 U.S.C. §§ 1431(b) and 1433(d), CBP has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. CBP has published extensive guidance for the travel industry in regards to APIS compliance. Guidance to voluntary APIS submission is available for Bus and Rail. *See* CBP Bus APIS Document Guidance, *available at* https://www.cbp.gov/sites/default/files/documents/cbp_bus_apis_doc_1_3.pdf and CBP Rail APIS Document Guidance, *available at* https://www.cbp.gov/sites/default/files/documents/apis_doc_3.pdf.

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM – VOLUNTARY RAIL AND BUS SUBMISSIONS (APIS-VRBS), DHS/CBP/PIA-001(d) (2009), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection, and DHS/CBP-005 Advance Passenger Information System (APIS), 80 Fed. Reg. 13407 (March 13, 2015), *available at* www.dhs.gov/systems-records-notices-sorns.

Screening and Vetting

Upon receipt, APIS data is immediately sent to other CBP enforcement databases, including TECS[10] and the Automated Targeting System (ATS)[11] for cross-referencing and storage. As part of this process, API is screened against internal CBP holdings and external databases including the Federal Bureau of Investigation (FBI) Terrorist Screening Center's Terrorist Screening Database (TSDB). APIS yields information on outstanding wants or warrants, and information from other government agencies regarding high-risk parties; enables CBP to confirm the accuracy of that information by comparison with information obtained from the traveler and from the carriers; and facilitates making immediate determinations as to a traveler's security risk and admissibility and other determinations bearing on CBP's inspectional and screening processes.

Reason for the PIA Update

The APIS PIA series previously only discussed mandatory air and commercial vessel API submissions, and voluntary rail and bus carrier API submissions, as well as the collection of the data elements outlined above. With this PIA update, CBP is formally documenting 1) the expanded collection and receipt of voluntary API in the air, land, and sea environments, including bridges and ferries; 2) the collection of expanded biographic data elements; and 3) the updated data retention period of 13 months.

Voluntary API - Land Border Crossings

There are several bridges that connect the United States to neighboring countries, Mexico and Canada. Some bridges require pedestrians or vehicles to pay a fee in the form of a toll or ticket in order to cross the bridge and enter into the United States. Upon publication of this PIA, CBP will begin accepting voluntary API submissions from certain entities, such as bridge operators, who require travelers to purchase tickets to cross a bridge into the United States.

Cross Border Xpress (CBX) Use Case

The CBX footbridge allows commercial air carrier passengers and crew arriving at Tijuana International Airport in Mexico the ability to enter the United States without exiting the airport in Mexico.[12] Travelers are charged a fee for using the CBX footbridge to cross into the United States.

---

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[11] *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.

[12] Cross Border Xpress (CBX) is a pedestrian bridge exclusively for passengers and crew of the Tijuana International Airport that allows passengers [and crew] to cross the border between Mexico and the United States. All passengers [and crew] can use Cross Border Xpress with a valid reservation or flight with any air carrier that

Only air passengers and crew arriving into the Tijuana International Airport and planning to cross the border to the United States may use the footbridge. The footbridge is not available to non-traveling individuals as they are not permitted to enter the sterile area of Tijuana International Airport to use CBX facilities.

Beginning in early 2021, CBP will begin receiving CBX traveler API voluntarily in two ways. Depending on the air carrier, when a traveler books a flight to Tijuana International Airport in Mexico, the traveler may be given the option to also purchase a ticket to use the CBX footbridge. If the traveler chooses to purchase a ticket in this manner, the air carrier will code the reservation appropriately and include the information in its regular API submission to CBP. In this scenario, air carriers submit the information using existing processes and connectivity with CBP, including direct submissions to the DHS Router or through the eAPIS web portal. Travelers also have the option of purchasing a CBX footbridge ticket upon arrival at the Tijuana International Airport. In this scenario, CBP will receive API using existing infrastructure.

Voluntary API – Ferries

In 2005, CBP issued a Final Rule[13] implementing the statutory mandates for commercial air and vessel carriers to submit API to CBP. Another Final Rule[14] was issued in 2008 for private aircraft pilots to submit API to CBP. CBP's regulation regarding commercial vessel API defines "commercial vessel" as "any civilian vessel being used to transport persons or property for compensation or hire."[15] The commercial vessel API requirement does not apply to ferries, which are defined as "any vessel which is being used to provide transportation only between places that are no more than 300 miles apart and which is being used to transport only passengers and/or vehicles, or railroad cars, which are being used, or have been used, in transporting passengers or goods."[16] Although ferry operators are not required to send API to CBP, ferry operators may voluntarily provide API for passengers and crew traveling by ferry to the United States. There are several ferry routes that connect the United States with other countries. If a ferry operator should choose to submit API to CBP, it is typically completed through eAPIS and treated like all other API received through eAPIS. CBP uses this API to conduct vetting prior to a traveler's arrival,

operates out of the Tijuana International Airport. The bridge is 390 feet long and connects the Tijuana International Airport with a service terminal in San Diego. CBX serves millions of travelers who cross the border as part of their travel, helping them avoid the more congested San Ysidro and Otay Mesa ports of entry. For more information, *see* https://www.crossborderxpress.com/en/. In 2015, CBP opened a new CBP inspection facility within the new passenger terminal on the U.S. side of the border. All travelers seeking to enter or depart the United States via Cross Border Xpress are subject to inspection by a CBP officer.

[13] 70 Fed. Reg. 17820 (April 7, 2005).

[14] 73 Fed. Reg. 68295 (November 18, 2008).

[15] 19 CFR 4.7b(a).

[16] 19 CFR 4.7b(a), (c)(1).

which also expedites the traveler's inspection process. Ferry operators may choose to establish direct connections to CBP as well.

Expanded Biographic Information

As described above, some carriers are required to send CBP certain passenger and crew manifest information to CBP APIS. CBP's regulations require commercial air carriers, commercial vessel carriers, and private aircraft pilots to provide a specified list of data elements, such as each passenger's name and U.S. address (address information is not required for U.S. citizens, lawful LPRs, or persons who are in transit). However, in addition to the mandatory data elements, carriers may voluntarily choose to submit additional non-required information to CBP via their APIS transmissions.

In December 2020, several air carriers opted to voluntarily send additional biographic information beyond what is required in the APIS regulations (e.g., passengers' phone numbers, secondary contact numbers, and email addresses) as part of expanded support to the Centers for Disease Control and Prevention's (CDC) public health response efforts as a result of the COVID-19 pandemic.

Air carriers choosing to submit this expanded information ask travelers to voluntarily provide additional contact information at booking/check-in. Upon collection, the air carriers submit the expanded biographic information to CBP with their standard APIS submissions.[17] In turn, CBP consolidates this information with other relevant contact and travel information found on the traveler in CBP holdings to create a person-centric record. CBP then provides this person-centric record 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).

Like all other APIS information, this expanded information is automatically sent to ATS immediately upon receipt. 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.

[17] Alternatively, air carriers may submit these elements to CBP directly through a JavaScript Object Notation (JSON) connection or through the air carrier's Passenger Name Record (PNR) submission.

CBP has published a comprehensive PIA entitled, "DHS/CBP/PIA-066 CBP Support of CDC for Public Health Contact Tracing" to describe CBP's efforts to support CDC in greater detail.[18]

While not mandated or in current practice, commercial and private air carriers, commercial vessel carriers, rail and bus carriers, or ferry operators may voluntarily choose to provide the same expanded data elements to CBP to support the CDC and CBP missions, respectively.

Retention

The previous APIS PIA series documented a 12-month retention period for APIS. With this PIA update, CBP is changing the retention period to reflect the retention of APIS records for 13 months. This is not an expanded retention period; rather CBP has historically retained information for 13 months and the prior documentation was incorrect.

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes to CBP authorities and other requirements with this PIA update. Although CBP is receiving voluntary API submissions from rail and bus carriers and ferry operators, as well as additional biographic information from certain carriers, CBP continues to rely on existing authorities to collect this additional data. The Aviation and Transportation Security Act of 2001, Pub. L. 107-71; the Enhanced Border Security and Visa Reform Act of 2002, Pub. L. 107-173; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; and the Tariff Act of 1930, Pub. L. 71-361, as amended, including 19 U.S.C. §§ 58b, 66, 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, and 1644a cover this collection. Additionally, CBP relies on the 42 U.S.C. § 268(b) to assist CDC, which states that it "shall be the duty of the customs officers to aid in the enforcement of quarantine rules and regulations."

The DHS/CBP-005 Advance Passenger Information System (APIS) System of Records Notice provides coverage for the collection and use of this information.[19] CBP is also in the process of updating this system of records notice (SORN).

APIS continues to reside on the TECS security boundary. The TECS ATO was renewed in December 2020.

OMB Control Number 1651-0088 continues to cover the collection of APIS information under the Paperwork Reduction Act.

---

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP SUPPORT OF CDC FOR PUBLIC HEALTH CONTACT TRACING, DHS/CBP/PIA-066 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[19] *See* DHS/CBP/PIA-001 Advance Passenger Information System, 80 Fed. Reg. 13407 (March 13, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

Characterization of the Information

CBP continues to collect and maintain the information previously outlined in the APIS PIA series. However, in addition to the previously collected information, CBP may also collect email addresses, addresses of all travelers while in the United States, travelers' phone numbers, and secondary contact phone numbers. Travelers are given the option to voluntarily provide this information to air carriers when making a flight reservation or while checking in for a flight. 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. Therefore, this expanded collection will result in CBP obtaining new information on U.S. citizens and LPRs.

CBP continues to collect information from the same sources but is also expanding the collection to receive API from bridge and ferry operators.

This update does not impact the use of information from commercial sources or publicly available information contained in non-social media internet sites.

This update does not impact the accuracy of the data. CBP assumes the information to be accurate, since the information is typically originally supplied directly from the individual and his or her travel document to whom the collection of information pertains.

There are no new privacy risks associated with the collection of voluntary API from bridge and ferry operators. Bridge and ferry operators send the same API that CBP has historically received from airlines, rail, and bus carriers. However, CBP identified the below risk associated with the collection of voluntary API.

Privacy Risk: There is a risk of over collection now that CBP is collecting additional data elements beyond what is included in the APIS regulations, including the expanded collection of information on U.S. citizens and LPRs.

Mitigation: This risk is partially mitigated. Travel operators begun providing and CBP began collecting this additional information to assist CDC in their public health response efforts, specifically as a result of COVID-19 contact tracing efforts. CDC determined that the expanded data elements (e.g., email address, U.S. address, and primary/secondary phone number) are critical data elements to effectively identify, monitor, and support travelers who have been exposed to, and possibly infected with a communicable disease, such as COVID-19. According to CDC, prompt identification, voluntary quarantine, and monitoring of exposed individuals can effectively break the chain of disease transmission and prevent further spread in a community.

As described above, upon receipt APIS data is immediately transmitted to ATS for storage. ATS 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.

CBP uses this information for vetting and targeting purposes to identify individuals who may need additional scrutiny. The limited amount of voluntarily-provided 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.

The additional data elements are currently limited to biographic data elements used to amalgamate data within CBP holdings and share, for example, with CDC to assist in public health related responsibilities. CBP Privacy and the CBP Office of the Chief Counsel (OCC) will work with CBP operators to carefully evaluate the collection and retention of any additional data elements beyond what is outlined in the APIS regulations and beyond the specified biographic information outlined above. CBP Privacy and CBP OCC will collaboratively ensure the collection and use aligns with the CBP mission. Finally, CBP will issue PIA updates, as necessary, to address additional privacy risks associated with the new information collections.

Uses of the Information

CBP will use the API sent by bridge and ferry operators in the same manner as API sent by air, vessel, rail, and bus carriers. Furthermore, although 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 upon request, CBP is now routinely providing CDC with contact information on all international travelers arriving in the United States by air and via land ports of entry (if available). Additionally, with this update, in response to the COVID-19 pandemic, CBP is currently sending expanded biographic contact information to CDC to increase the chance of successfully contacting a traveler and ultimately assist the CDC in reducing the spread of COVID-19.

There are no new privacy risks associated with the use of voluntary API received from bridge and ferry operators. However, CBP identified the below risk associated with the use of voluntary API.

Privacy Risk: There is a risk that CBP is using this information for purposes beyond the reason for which it was originally collected.

Mitigation: This risk is mitigated. CBP uses this information in support of traveler screening and vetting, law enforcement, border security, public security, counterterrorism, and national security missions, as appropriate. In addition to the CBP uses, CBP shares this information with external entities pursuant to Routine Uses in the APIS SORN. For example, pursuant to Routine Use L in the APIS SORN, CBP shares this information with CDC to use for public health response efforts. CDC provides the contact information for exposed travelers to state and local health authorities to perform contact tracing, as appropriate. These entities 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).

Notice

CBP is providing notice of these changes through the publication of this PIA. The original collection of API is completed by the carriers and operators. Therefore, CBP places the responsibility on these entities to supply notice to the traveler on the collection of API and how the carriers/operators intend to transfer that information to the U.S. Government. Carriers and operators typically provide notice of this collection and transfer on their travel booking websites and within their privacy policies. Furthermore, CBP has separately published a comprehensive PIA entitled, "DHS/CBP/PIA-066 CBP Support of CDC for Public Health Contact Tracing,"[20] documenting the expanded collection of biographic information via APIS to assist in CDC's public health response efforts. There are no additional risks to notice outside of the risks previously documented in the APIS PIA series and the DHS/CBP/PIA-066 CBP Support of CDC for Public Health Contact Tracing.

Data Retention by the Project

The previous APIS PIA series documented a 12-month retention period for APIS. With this PIA update, CBP is updating the retention period to reflect the retention of APIS records for 13 months.

Privacy Risk: There is risk that CBP is retaining APIS data for longer than necessary, since CBP transmits and stores the data in both ATS and TECS.

[20] *See supra* note 18.

Mitigation: This risk is partially mitigated. CBP is publishing this PIA in part to accurately reflect a 13-month retention period. This is not an expanded retention period, rather CBP has historically retained information for 13 months but had not previously updated the PIA series to reflect this. Furthermore, while APIS only retains information for a limited period of time, all or a portion of APIS data is immediately transmitted to ATS, TECS, and the Arrival and Departure Information System (ADIS)[21] upon receipt. APIS information is ingested into ATS, ADIS, and TECS and is stored in those systems for 15 years and 75 years, respectively. Justification for a 15-year retention period in ATS 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. 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 in TECS. TECS and ADIS records are retained for 75 years from the date of the collection or for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Information Sharing

While CBP has historically shared APIS data with CDC on a case by case basis when requested by CDC, CBP is now shifting the way in which CBP will provide support for public health related purposes in response to the current COVID-19 pandemic. CBP is now building person-centric records using certain information found on travelers in CBP holdings. CBP then provides these 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. Routine Use L of the APIS SORN permits CBP to share APIS data with CDC 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

[21] *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.

transmission of a communicable or quarantinable disease or for combating other significant public health threats; appropriate notice will be provided of any identified health threat or risk. Furthermore, once APIS data is ingested into other systems (e.g., ATS, TECS, and ADIS) CBP permits APIS data to be shared with external entities in accordance with the applicable Routine Uses in those SORNs. CBP does not share API with external entities without a valid Routine Use (or as otherwise permitted by the Privacy Act of 1974, 5 U.S.C. § 552a) or information sharing agreement in place.

There are no additional privacy risks associated with information sharing related to this PIA.

Redress

There are no changes to redress as a result of this update.

Auditing and Accountability

There are no changes to auditing and accountability as a result of this update.

Contact Official

John Maulella
Director, External Engagements and Initiatives
Office of Field Operations
U.S. Customs and Border Protection
202-344-2605

Responsible Official

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

Approval Signature

Original, signed copy on file with DHS Privacy Office.

_____

James V.M.L. Holzer
Acting Chief Privacy Officer
U.S. Department of Homeland Security