Privacy Impact Assessment Update
for the
Advance Passenger Information System (APIS): Land Pre-Arrival System (LPAS) for Bus and Rail

DHS/CBP/PIA-001(h)

December 13, 2019

Contact Point
John Maulella
Director, Traveler Entry Programs
US Customs and Border Protection
(202) 344-2605

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

Abstract

U.S. Customs and Border Protection (CBP) uses advance passenger information (API) to ensure the security of legitimate passengers and fulfill its border security mission. CBP has collected mandatory and voluntary 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 document the Land Pre-Arrival System (LPAS) mobile application and conduct a privacy risk assessment of this new method for rail and bus carriers to voluntarily submit API to CBP.

Overview

CBP, pursuant to existing regulations,[1] currently requires commercial air and vessel carriers and private aircraft pilots to provide CBP with personally identifiable information (PII) about passengers and crewmembers traveling by air or sea and arriving in and/or departing from (and, in the case of aircraft crew, overflying) the United States. This information, often collected and maintained on what is referred to as the passenger manifest, can be found on routine travel documents that passengers and crew members must provide when processed into or out of the United States; most of the information is included on the Machine Readable Zone (MRZ) of a person's passport. Once collected, the information is transmitted to CBP through the Advance Passenger Information System (APIS), an electronic data interchange system used by DHS for international commercial air and vessel carriers and for advance information transmitted to CBP by private aircraft pilots.

Using advance passenger and crew information, CBP is able 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 travel safety or to national or public security, or of non-compliance with U.S. civil and criminal laws, while simultaneously facilitating the travel of legitimate passengers and crew members.

Voluntary APIS Submissions

Under 19 U.S.C. 1431(b), CBP has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. In addition to the mandatory submissions provided

[1] CBP's APIS regulations include 19 CFR 4.7b, 4.64, 122.22, 122.49a, 122.49b, 122.49c, 122.75a, and 122.75b.

by both commercial air and vessel carriers and private aircraft pilots, CBP receives voluntary APIS submissions from rail and bus carriers.[2] 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 all rail and bus traffic crossing the border.

Private and commercial rail and bus carriers can submit passenger and crew manifests to CBP via direct system connections or through the Electronic Advance Passenger Information System (eAPIS) web interface.[3] 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 information. Passenger information successfully submitted into the eAPIS web interface and received by CBP is stored as Advance Passenger Information System (APIS) data.[4]

The voluntary bus/rail APIS program began after air carriers and vessels were mandated to provide API to CBP prior to arrival in the United States. In order to keep security processes similar in the land environment, CBP developed a voluntary program for bus/rail. The voluntary program allows bus and rail carriers to submit traveler manifest data, gathered from the information travelers provide, into eAPIS, the CBP APIS web portal. Oftentimes, the information bus/rail carriers provide to CBP is incomplete or inaccurate, causing CBP officers to update the manifest upon inspection or not use the manifest for processing at all. This has resulted in limited submissions of API by bus and rail carriers and limited usage of bus and rail API by CBP to facilitate processing. Due to the limitations of the current voluntary program, CBP has been unable to evaluate the effectiveness of API in the bus and rail environment.

Bus Submissions

Presently, private bus carriers voluntarily submit bus manifest data into eAPIS and manually enter it. CBP established a program of unique carrier codes to issue to private bus carriers for electronic submission via eAPIS. The unique carrier code permits private bus carriers to voluntarily submit advance passenger and crew information to CBP. The carrier code is used when creating an eAPIS account. eAPIS submission accounts have been created for 31 different bus

[2] 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.

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

[4] *See* DHS/CBP/PIA-001(d) Advanced Passenger Information System-Voluntary Rail and Bus Submissions (APIS-VRBS), (Feb 19, 2009), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_apis_vrbs_0.pdf, and DHS/CBP-005 Advanced [*sic*] Passenger Information System (APIS) System of Records Notice (SORN), 80 FR 13407 (March 13, 2015).

carriers and/or their third-party submitters. This data is generally received by CBP before a bus departs from either a Mexican or Canadian location for the United States.

In addition to the eAPIS submission process, bus carriers and/or their third-party submitters can choose to enter and submit manifest data into the LPAS mobile application. The assigned carrier code and sender ID[5] are required to create an account in the LPAS mobile application and login.gov.[6] Login.gov is a service that officers secure and private online access to government programs, such as federal benefits, services, and applications. Login.gov manages user authentication by allowing users to sign in with an email address, password, multi-factor method, and identity proofing by verifying an individual's asserted identity on behalf of partner agencies. Individuals with a login.gov account can sign in to multiple government websites (including LPAS) with the same email address and password.

CBP provides both the carrier code and sender ID to carriers. The carrier code and sender ID are an additional layer of security used to authenticate the bus carrier employee into the LPAS mobile app. Without the carrier code and sender ID, the bus carrier employee cannot access the LPAS mobile application. All data collected in LPAS is transmitted to APIS.

LPAS allows the carrier to capture and upload data through an automated process, using the machine readable zone (MRZ) reader embedded into the application. Only in specific cases will the MRZ reader not work on the document (i.e., a minor child traveling with a non-Western Hemisphere Travel Initiative document, a tribal card holder); in those cases, the carrier must manually enter the passenger data (as it does now) into the application and it will be forwarded to CBP electronically.

Rail Submissions

Rail carriers operating trains that cross the U.S. border with either Mexico or Canada are subject to part 123 of Title 19 of the Code of Federal Regulations. Part 123 includes provisions governing how carriers report arrival and manifests. Pursuant to 19 CFR 123.1, rail carriers are required to make a report of arrival to CBP for any train arriving in the United States from a foreign location, which must be made upon arrival of the train at a U.S. Port of Entry (POE). Individuals arriving in the United States from a foreign location must also report their arrival to CBP once they arrive in the United States.

Similar to bus manifest submissions, rail carriers currently receive unique carrier codes that are used with eAPIS. Passenger and crew information is collected upon train ticket purchase and sent by the rail carriers to CBP upon train departure for the United States. Carriers submit the

[5] When the Office of Field Operations creates carrier codes they also create Sender Accounts for individuals who use the carrier codes. Sender accounts are identified by a unique code referred to as the Sender ID, which is used to identify the user who sent the manifest.
[6] *See* GSA/PIA-Login.gov, (August 26, 2019), *available at* https://www.gsa.gov/cdnstatic/Logingov_PIA_August2019.pdf.

information via eAPIS or by fax. The CBP LPAS mobile application will allow rail carriers and/or their third-party submitters to enter their carrier code and sender ID into the LPAS mobile app and login.gov. CBP provides both the carrier code and sender ID to carriers. The carrier code and sender ID are used to authenticate the rail carrier employee into the LPAS mobile app. Without the carrier code and sender ID, the rail carrier employee cannot access the LPAS mobile application. All data collected in LPAS will be transmitted to APIS.

Reason for the PIA Update

CBP is updating the previously published DHS/CBP/PIA-001(d) Advanced Passenger Information System-Voluntary Rail and Bus Submissions (APIS-VRBS) PIA, dated February 2009, to discuss a new method for rail and bus operators to voluntarily submit API to CBP. CBP is piloting a mobile option for reporting carrier manifest information to CBP for the bus/rail environment. Manifest submission for bus/rail continues to be voluntary. For this pilot, CBP will leverage the existing CBP Reporting Offsite Arrival-Mobile (ROAM) application[7] to include an option for bus/rail carriers to report U.S. entry to CBP via their smart device or tablet.

CBP is currently developing a stand-alone LPAS mobile application.[8] LPAS will collect and process all pre-arrival bus and rail manifest information to the designated U.S. POE selected by the bus and rail carrier prior to arrival. CBP Officers will access the manifest data submitted to CBP and use it to make informed admissibility and enforcement decisions prior to passenger arrival.

For this initial pilot phase, bus and rail carriers will access LPAS via the existing CBP ROAM mobile application. In order to use CBP ROAM, carrier employees have to create a login.gov account,[9] which is used to log in to CBP ROAM and verify credentials. To create a login.gov account, the carrier employee provides a valid email address as the user ID and a phone number for security authentication. The carrier employee then creates a password for log-in.[10]

Once the carrier employee has obtained login.gov access, that employee will be able to enter the CBP ROAM mobile application. CBP has added a "transportation" option listed on the drop-down screen, to allow carrier employees to select their mode of travel (i.e., bus or rail). This

[7] A PIA for the ROAM mobile application itself is forthcoming.
[8] ROAM is only to be used as a temporary platform for bus and rail manifest data collection. The bus and rail carrier functionality in ROAM will be decommissioned when the stand-alone mobile application, LPAS, is deemed operational.
[9] *See* GSA/PIA-Login.gov, (August 26, 2019), *available at* https://www.gsa.gov/cdnstatic/Logingov_PIA_August2019.pdf
[10] Carrier employees who do not have a login.gov account should create an account. Carrier employees who already have a login.gov account should sign into their existing account, and then they will be directed back to the CBP ROAM app.

option is available to anyone who accesses the CBP ROAM application; however, CBP will accept manifest submissions only from those carriers authenticated with a carrier code as part of their user profile.

After log-in, bus and rail carrier employees select the bus or rail option to begin the manifest submission process. Carrier employees are prompted to input their manifest information (i.e., passengers biographic information, conveyance, and trip details), and then submit to CBP. All information submitted into LPAS is sent directly to CBP APIS in the same manner as the eAPIS web portal submission process. For the initial launch, only carriers at the northern border will be able to use LPAS. CBP anticipates implementing LPAS for the southern border in the future.

Notice

Carriers participating in the pilot are responsible for notifying each passenger about information collected prior to arriving at a U.S. POE. Carriers must inform each passenger that the information collected in the LPAS mobile application will be transferred to CBP. Since the passengers do not have access to use the LPAS mobile application, providing passengers notice at the time of collection provides transparency and provides passengers an opportunity to consent to this data collection.

Upon passenger presentation at the departure location, the carrier will use a tablet or smartphone device to scan the Machine Readable Zone (MRZ) of a passenger's passport using the camera functionality within LPAS. The LPAS functionality produces a scan of the passport MRZ to populate the text fields within the LPAS submission screen but does not take a photograph of the travel document and does not store any information on the device or in the application. Once the carrier employee has scanned the MRZ of travel documents (or manually entered the information, if necessary) into LPAS for each passenger, the carrier employee will submit the manifest to CBP via the tablet or smartphone. As previously noted, no data is stored within the application, nor is it stored locally on the device.

After submission, CBP uses the information on the manifests to vet passengers prior to arrival and display results to CBP Officers.

Location-based information

In order to prevent fraudulent use of LPAS and provide operational awareness to CBP Officers, CBP ROAM captures GPS location at the time of manifest submission to CBP. CBP Officers use the location information to verify a carrier's self-reported anticipated POE and ensure CBP personnel are positioned appropriately to conduct inspections. In addition, the GPS location is a requirement that allows the receiving POE to gather an estimate on the amount of time they have to vet passengers before they arrive at the designated POE. This information is necessary to

CBP as it provides the opportunity for the POE to allocate resources to process the bus or rail entry into the United States.

Employees working for bus/rail carriers must enable location services on their mobile device before entering information into LPAS. The application will not work without turning on the device's location-based services. LPAS uses a geofencing feature that is set at 250 miles north of the United States/Canadian border. In order for the manifest data to be transmitted from the user's mobile device to CBP APIS, the user's mobile device must be within the 250-mile radius. LPAS only captures location information at the exact time of bus/rail operator's submission. CBP officers have access to view a GPS map on the dashboard. The map displays a blue dot only; LPAS does not display the GPS coordinates or address of the carrier, employee, or bus/rail location in the mobile application. The location of the bus/rail operator is not tracked beyond the time of submission of the data.

Location information also assists CBP in identifying fraudulent use of the application. CBP officers will use the map location to determine if submission locations are actually known bus stops. CBP will be able to detect "spoofing" techniques that alter the location of the device. CBP is able to determine if the point of origin is accurate. If not accurate, the CBP officer can contact the carrier via phone to gather the correct data.

Privacy Impact Analysis

Authorities and Other Requirements

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

Characterization of the Information

The information collected from passengers and crew members by rail and bus carriers for transmission to CBP via LPAS remains the same as the current process under eAPIS and as previously described and analyzed in full in the 2009 voluntary bus and rail APIS submissions PIA.

In addition to the previously published data elements described in the 2009 PIA, the LPAS mobile application (1) captures the GPS location of the carrier employee mobile device at the time the passenger manifest is submitted from the device, and (2) relies on General Services Administration (GSA) login.gov to authenticate carriers to the mobile application.

Location-based services are mandatory, and carriers must agree to permit the LPAS mobile application access to their device's location-based services/GPS prior to entering the mobile application. CBP deletes location information from LPAS after the bus or train is cleared through

the POE. GPS location information captured from the carrier at the time of manifest submission is not sent to APIS.

Uses of the Information

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

Notice

The method of collecting voluntary APIS information from bus and rail carriers is changing, however the risks to notice that exist with all API remain the same. CBP does not provide explicit notice to bus and rail passengers at the time of collection. Carriers submit API via LPAS in the same manner they submitted information using eAPIS. Individual passengers cannot log in and use LPAS to submit their own information to CBP. Individuals may decline to provide the requisite API prior to boarding the train or bus, however they may be subject to action by the carrier and be in violation of carrier terms of service or contract of carriage.

Privacy Risk: There is a privacy risk to notice since the carriers will use a tablet or smartphone device to scan the MRZ of a passenger's passport or travel document; passengers may be unaware that the collection is done on behalf of CBP.

Mitigation: This risk is partially mitigated. Typically, the carriers provide notice that an appropriate travel document is required as part of international travel, and they will deny a passenger the ability to board if a passenger does not possess a valid travel document. Passengers are required to have all travel documentation prior to admission into the United States. However, there a risk that passengers will be unaware that the carrier is submitting their travel document information in advance to CBP. As all passengers are required to provide CBP a valid travel document prior to admission into the United States, most (if not all) passengers on an international bus or rail conveyance are aware that CBP will review their identification documents.

If a carrier does not choose to participate in the voluntary APIS submission process, bus and rail passengers are still required to provide their information once they have arrived at a U.S. POE.

Data Retention by the Project

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

Information Sharing

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

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.

Responsible Official

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

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

Approval Signature

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

_____

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