U.S. Customs and Border Protection

Enhanced Passenger Processing

Business Requirements Document

Version 1.1
June 2025

APPROVALS

Jody M. Hardin
Executive Director
Innovation and Strategy Directorate
Office of Field Operations
U.S. Customs and Border Protection

Revision Summary

Version	Date	Editor	Remarks
1.0	03/26/2024	Biometrics Program Office	Initial Draft
1.1	06/04/2025	Biometrics Program Office	Update to Section 4.2, deleted reference to other seaports.

This Page Intentionally Left Blank

Table of Contents

Contents

1. Introduction

1.1 Background

U.S. Customs and Border Protection (CBP) is congressionally mandated to implement a comprehensive biometric entry-exit system.[1] In 2017, CBP developed a public-private partnership approach where-in stakeholders can incorporate biometrics into their respective operations. CBP offered stakeholders, also known as business sponsors, an "identity-as-a-service" solution that uses facial comparison technology to automate manual identity verification and complies with the congressional mandate for biometric entry-exit.

CBP's Traveler Verification Service (TVS) serves as the "identity-as-a-service" and the backbone of all CBP's facial biometric matching. TVS uses facial comparison technology in a cloud environment to match live traveler photos with photos maintained in U.S. government holdings. The biometric entry-exit program is designed to facilitate a public-private partnership wherein business sponsors procure and maintain biometric equipment that uses TVS to fulfill the biometric entry-exit requirements efficiently and effectively. These public-private partnerships enable CBP to deploy large-scale transformation that will facilitate travel, while making it more secure, in fulfillment of Department of Homeland Security (DHS) mission responsibilities

While public-private partnerships are primarily leveraged for outbound passenger processing, there are instances in which CBP partners with stakeholders to process inbound travelers. Enhanced Passenger Processing (EPP) is one of these circumstances. Inbound traveler volumes continue to increase, while personnel remain the same. Because of this, CBP relies on innovation and technology. EPP is an innovative, modified primary inspection process that allows interested business sponsors to procure stand-alone biometric capture devices to be used by CBP. The process is limited to certain citizenships and classes of admission determined by CBP and is designed to facilitate the inspection and adjudication of low-risk travelers entering the United States while enhancing security by allowing the CBP officer to focus on the traveler interaction. CBP can then better utilize resources and officers can focus more on higher risk travelers.

1.2 Purpose

This document identifies the business requirements for partner cruise lines, port authorities, airlines, and/or airport authorities to participate in EPP. Additionally, this document provides a list of operational recommendations that should be accounted for when onboarding new sites.

[1] The following statutes require DHS to take action to create an integrated entry-exit system: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337; Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106- 396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, 353; Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, 130 Stat. 122, 199.

2. Acronyms

Term	Definition
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
EPP	Enhanced Passenger Processing
FIPP	Fair Information Practice Principles
ICD	Interface Control Document
PIA	Privacy Impact Assessment
POE	Port of Entry
RTM	Requirements Traceability Matrix (DHS Security Requirement)
TVS	Traveler Verification Service

3. Business Requirements

This section describes the business requirements for EPP at an air or sea port of entry. EPP is an approved TVS use case. The business requirements are applicable to the business sponsor and vendor. The business requirements are in conjunction with the Interface Control Document (ICD) provide by CBP.

#	Requirement	Comments
1	The business sponsor and its vendor(s) must adhere to the requirements outlined in this document and the ICD.	A business sponsor must be a partner cruise line, port authority, airline, and/or airport authority.
2	The business sponsor must return a signed copy of this document's acknowledgement and compliance page, which confirms receipt of the program's business requirements and records the business sponsor's agreement to comply with the requirements. When an updated version of these requirements has been promulgated, the business sponsor must sign and return the updated version within 30 days of receipt. The EPP BRD is a separate and unique document from other CBP BRDs and requires its own signature.	Any EPP-related contract between a business sponsor and another organization (e.g., a systems integrator, vendor, or other third party) must detail the specified actions and measures that will be taken to ensure compliance with all relevant business requirements contained herein and technical requirements contained in the ICD.
3	The business sponsor and CBP must mutually agree on the use of EPP at a given location. The business sponsor is responsible for procuring, supporting, maintaining, and monitoring the hardware, software, and network connection to the EPP webservice. The business sponsor must provide CBP with the camera's manufacturer information, including name, model, serial number, and firmware version.	CBP may request additional IT and security documents from the business sponsor. Examples may include but are not limited to the DHS Security Requirements Traceability Matrix (RTM); and/or the Federal Risk and Authorization Management Program (FEDRAMP) certification. Requirements can be found at fedramp.gov. All CBP requests for security documentation must be fulfilled and approved prior to "Go-Live" and connectivity with CBP's production environment.
4	The business sponsor and its vendor must adhere to the CBP prescribed naming convention for device unique identifiers (i.e., camera's "Device_ID"). The scheme should comply with the following: (1) Port; (2) Terminal;	If the vendor recommends a different approach, CBP will consider all requests.

	(3) Berth; (4) Camera Model; and (5) Camera number. An example Device_ID is ATL-E-014- Vendor-01.	
5	The business sponsor must provide the required power for all hardware.	
6	The business sponsor must provide, if not already available, reliable, secure, and external high- speed internet access. A hard-wired connection is preferred, but high-speed wireless will be adequate if the connection can be made reliable.	CBP recommends the following: A Wi-Fi 5 or Wi-Fi 6 router with client device connections on a 5GHz band. Wi-Fi extenders placed close to the hardware to ensure coverage.
7	The business sponsor and all relevant third parties (e.g., cruise lines and port authorities) must comply with applicable DHS/CBP security and privacy policies and compliance documentation. Business sponsors and participating organizations should ensure their own privacy policies and notices are updated. CBP will conduct compliance reviews on a periodic basis.	The TVS Privacy Impact Assessment (PIA) contains a complete list of applicable privacy practices (e.g., posting DHS-branded, clearly visible signs in close proximity of and prior to the cameras, and facilitation of exemption processing for travelers who elect to opt-out). All notices and signage created by business sponsors must be reviewed and approved by CBP prior to "Go-Live" and connectivity with CBP's production environment. The current TVS PIA, along with the applicable appendices and its predecessor PIAs, can be found at: www.dhs.gov/privacy
8	Any photos taken through the EPP process must not be stored and/or retained by the business sponsor or its vendor. The business sponsor and the sponsor's vendor must provide a mutually agreeable method by which CBP is able to audit compliance with this requirement.	
9	Any public communications regarding EPP and/or EPP performance or CBP's biometric entry-exit program must be coordinated with CBP prior to release to the public or media. Any marketing campaigns, multimedia content, or disclosures related to CBP, EPP, TVS, or the biometric entry-exit program must be approved in advance and in writing by CBP.	Public releases that do not reference CBP or any of its programs and systems (such as EPP and TVS) do not require CBP coordination or approval. Public releases that do reference CBP or any of its programs and systems should be coordinated as soon as possible. CBP

		recommends at least 7 days in advance to ensure prompt approval.
10	The hardware needs an officer/agent notification mechanism to ensure the operators are informed of the CBP system results: (1) No Match, (2) Recapture or Error/Issue, and (3) Match. The three result messages/notifications must be distinctly differentiated and clear to the operator. If providing visual cues the colors should be: Blue: No Match/Referral Green: Match/Release Yellow: Error/Poor Photo If providing some other notification mechanisms (e.g. dashboard, rear facing monitor), the messaging must be clear, concise, and easy to understand.	It is imperative for the operator to identify system results to determine a course of action. If a traveler is a no match, that result indicator will lead to one set of activities where poor image quality or facial capture indicators will lead to a different set of activities.
11	Transactional data, to include unique IDs and matching results received, may be retained but MUST be deleted within 180 days. All data must be encrypted at rest and in transit.	The log files and data are subject to select privacy and security policies depending on their content, retention period, and purpose. As specified above, all photos captured must be immediately deleted once the transaction is complete.
12	CBP must be allowed to review and/or assess any retained or derived data, code, encryptions, network connections and any other EPP or TVS related technical specifications.	
13	The business sponsor must coordinate with CBP to ensure that CBP- approved privacy signage is posted at each location. The signage must be clearly visible and placed at a sufficient distance in front of the camera to provide the traveler with a reasonable opportunity to read the content and opt- out before reaching the photo capture area.	Signage Requirements: Signage should be at least 22 inches wide and 28 inches tall. If signs meet this requirement, only one sign needs to be present at each processing location. If signage is smaller than 22 inches wide and 28 inches tall, a minimum of two signs need to be present unless accompanied by e-signage.

14	Upon the identification of a system performance, security, or other issue, the business sponsor and vendor must provide a detailed remediation plan and schedule. The business sponsor will provide progress reports to the CBP Biometrics Program Office on a mutually agreed-upon interval.	All remediation schedules must be completed as quickly as possible.
15	CBP must be notified of any cybersecurity-related incidents or breaches that occur on networks and hardware maintained by the business sponsor as part of the EPP process. All known or suspected incidents or breaches shall be promptly reported to the CBP Biometrics Program Office, CBP Privacy Office, and CBP Security Operations Center within 24 hours after discovery of a suspected incident or within 1 hour after a suspected incident has been confirmed, whichever is earlier.[2]	This requirement begins as soon as the process is operational. Points of Contact: • Biometrics Program Office: BPO@cbp.dhs.gov • CBP Privacy Office: privacyincidents@cbp.dhs.gov • CBP Security Operations Center: CBPSOC@cbp.dhs.gov Source: DHS Privacy Incident Handling Guidance (https://www.dhs.gov/publication/privacy-incident-handling-guidance-0)
16	The business sponsor and/or vendor must ensure that all access to the software or hardware used as part of EPP is secured and restricted to authorized personnel only. CBP does not permit any unsecured methods of externally accessing the camera (e.g., interfaces or ports such as USB). Furthermore, access to the system and its endpoints must require no less than a username/log-in and password.	
17	The business sponsor's system must be designed to include a time-out mechanism for each camera when not in active use for passenger processing operations.	The "time-out" feature should minimize any unintentional photographs taken of non-travelers.

[2] DHS defines a "privacy incident" as the following: "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than the authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses [PII] for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm." For more information, please see the DHS instruction guide 047-01-008, Privacy Incident Handling Guidance, *available at* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.

18	All maintenance of the equipment and software development provided by the business sponsor or relevant stakeholder in support of EPP is the responsibility of that business sponsor and/or the relevant participating stakeholders. Any personnel with access to equipment that is located within a secured area must meet port security requirements for access to secured areas. Port security screening requirements may include criminal history, background, and fingerprint check and CBP vetting.	
19	The business sponsor and vendor may not use any equipment to collect and send data to TVS, which has been manufactured by, or has parts that have been manufactured by, any company that is banned by statute or regulation from being purchased by a Federal Government agency or is suspended or debarred for federal contracts. This includes Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 and the System for Award Management (SAM).	The List of Equipment and Services Covered by Section 2 of The Secure Networks Act: List of Covered Equipment and Services. The list identifies equipment produced by particular entities that constitutes "covered" equipment such as video surveillance and telecommunications equipment. Companies including ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Huawei, or Dahua Technology Company (or any subsidiary or affiliate of such entities), whom the Federal Government is banned from using for national security reasons.
20	All relevant business sponsor and system integrator personnel are required to review the Fair Information Practice Principles (FIPPs).	The FIPPs provide the foundational principles for privacy policy and implementation at DHS and its components. Please see Appendix B for a list of the DHS FIPPs.

4. Operational Considerations and Recommendations

This section describes the operational considerations for partners participating in Enhanced Passenger Processing at air and sea ports of entry.

#	Requirement	Comments
1	The business sponsor must secure approval for deployment from local CBP and the CBP Biometrics Program Office.	
2	EPP Pre-inspection is designed to allow United States Citizens, Lawful Permanent Residents, and Canadian Citizens travelling as Visitors for Pleasure (B2) to utilize the process. The port of entry, port authority, airport, airline, and/or cruise line staff must ensure that any no match or individual that cannot be processed is directed to a CBP officer for processing. This includes any Canadian citizen not travelling as a B2 visitor.	This process is specific to Vancouver. EPP defaults the class of admission for Canadian Citizens to B2 and an I-94 will be issued for 6 months. Any other class of admission must be processed by a CBP Officer through Simplified Arrival-Sea.
3	Only eligible citizenships and/or classes of admission are permitted to use EPP. All other class of admission must be processed by a CBP officer through Simplified Arrival.	Port authorities, air and sea carriers, terminal operators, etc. are responsible, in coordination with local CBP, for queuing and ensuring the appropriate individuals pass through EPP. CBP officers manning or monitoring EPP hardware have the option to ask questions to each EPP user, as appropriate.
4	In accordance with existing practices, all locations using EPP must ensure notices are provided that United States Citizens may opt out of the process.	Proper privacy and opt out signage in advance of the queuing line and staff messaging provides the traveler the opportunity to read the signage and opt out, if they choose.
5	To ensure all photo galleries for matching purposes are available to the EPP process, the business sponsor must work with the relevant parties to ensure all vessel or aircraft schedules, diversions, delays, and arrival/departure times are updated within the relevant systems as soon as possible.	If a vessel or aircraft is significantly delayed without a corresponding update with a new departure time, biometric entry-exit processing/boarding may not be available.

Acknowledgement and Compliance Declaration

I, _____, acknowledge that I have received and read the Enhanced Passenger Processing Business Requirements Document (BRD) and Interface Control Document on behalf of

_____ and agree to comply with the contents as of the date of signature.

Signature: _____

Name: _____

Title: _____

Date: _____

Appendix A: DHS Fair Information Practice Principles (DHS FIPPS)

CBP adheres to the following privacy principles when operating biometrics:

Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements[3].

[3] *Privacy Policy Guidance Memorandum*, Hugo Teufel III, Chief Privacy Officer, U.S. Department of Homeland Security (Dec. 29, 2008), www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Appendix B: Image Quality Requirements

A facial recognition quality photo shall have reasonable compliance with the American National Standards Institute (ANSI)/ The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) -ANSI/NIST ITL 1-2011 Type 10 standards and subject acquisition profile levels 10-20 for frontal images, with the only allowable departure from the standard's requirements being the presence of mild pose variations around frontal.

The photo shall include the following characteristics:

1. A JPEG or JPEG 2000 file of no more than 150KB
2. Minimum resolution of 480 pixels by 760 pixels
3. A distance of at least 80 PX between the eyes
4. Eye roll of no more than 30 degrees
5. A front-facing photograph with:
    a. Tilt, no more than ± 5%
    b. Roll, no more than ± 15%
    c. Pan, no more than ± 15%
6. Uniform Illumination
    a. Exposure
        i. The average of 8-bit RGB components within each area shall fall between 105 and 125 with a standard deviation of ± 10. Furthermore, for every area examined, the maximum difference between the means of any two of the RGB components shall not exceed 10
        ii. By examining the histogram of the image, the RGB code value for a minimum of six gray patches should fall within range from 0.5 to 1.5 neutral density
    b. Saturation
        i. For each patch of skin on the person's face, the gradations in texture shall be clearly visible. There shall be no saturation (over or under exposure) on the face.
        ii. The Δ E 1976 of each color for the sRGB color space is to be less than 10 with CIELab (L*a*b*) value
7. No grayscale photos
8. Minimal Noise
    a. Peak Signal to Noise Ratio must be greater than or equal to 53 dB
    b. Minimal Blur
        i. Photos with defocus blur approximating Gaussian blur must have a radius of less than 4 sigma
        ii. Photos with motion blur must have a measured displacement of less than 9 pixels