U. S. Customs and Border Protection

Biometric Sea Entry-Exit Business Requirements

Version 2.0

June 27, 2023

Approvals

Approved by:

Matthew S. Davies
Executive Director
Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection

Revision Summary

Version	Date	Remarks
1.0	May 13, 2021	Initial draft developed
2.0	June 27, 2023	Updated

This Page Intentionally Left Blank

Table of Contents

1. Introduction

1.1 Background

U.S. Customs and Border Protection (CBP) is congressionally mandated to implement a biometric entry-exit system.[1] In 2017, CBP developed a public-private partnership approach to a comprehensive biometric entry-exit system that stakeholders can incorporate 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) offers a process for compliance with the pre-departure clearance of passengers under the Intelligence Reform and Terrorism Prevention Act. TVS uses facial comparison technology in a cloud environment to match live traveler photos with photos maintained in U.S. government holdings. Stakeholder participation in biometric entry-exit is voluntary and is not mandated by CBP. Furthermore, 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 efficiently and effectively fulfill the biometric entry-exit requirements for in-scope passengers.[2] Through partnerships with various business sponsors, CBP is enabling a large-scale transformation that will facilitate travel, while making it more secure, in fulfillment of DHS mission responsibilities.

1.2 Purpose

This document identifies the business requirements for partner cruise lines and seaport authorities to participate in biometric entry (debarkation) and exit (embarkation) and other CBP approved TVS use cases. Additionally, this document provides a list of operational recommendations that should be accounted for when onboarding new sites. This harmonizes the data collection and privacy standards each stakeholder must follow.

---

[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] An "in-scope" traveler is any person who is required by law to provide biometrics upon exit from the United States pursuant to 8 CFR 235.1(f)(1)(ii). In-scope travelers include any aliens other than those specifically exempt as outlined in the CFR.

2. Definitions

Term	Definition
Biometric Confirmation Rate	The percentage of all travelers on a given vessel who were biometrically confirmed.
Technical Match Rate	The percentage of in-scope travelers with a valid encounter photo and a gallery photo available for matching, who were successfully matched by TVS.
Capture Rate	The percentage of in-scope travelers whose encounter photo taken at crossing was of sufficient quality to be submitted and accepted by TVS for matching purposes.
Photo Gallery	A compilation of government holding photos, specific to a manifest, used for facial comparison. Photo galleries are templatized and stored in a cloud environment for matching.
Gallery Completion Rate	The percentage of travelers who had a gallery photo available for matching.
Exception Processing Required	Passenger needs manual processing. Please see Operational Considerations in Section 4 for additional instructions.

3. Business Requirements

This section describes the business requirements for biometric sea entry-exit and approved TVS use cases. The term 'system' in Section 3 refers to any physical equipment, software and/or any resource involved in the biometric sea entry-exit process or approved TVS use case.

#	Requirement	Comments
1	The business sponsor and its systems integrator must adhere to the requirements outlined in this document and the technical on-boarding guide attached as Appendix A.	A business sponsor must be a partner cruise line and/or port authority that facilitates the use of TVS to implement biometric entry-exit.
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. Once an updated version of these requirements has been promulgated, the business sponsor must sign and return the updated version within 30 days of receipt.	Any TVS-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 Reference Guides (TRG).
3	The business sponsor and its systems integrator must submit and receive approval for a proposal, which incorporates the use of TVS. For approval, the business sponsor is required to submit information including network topology, high-level solution architecture, test schedule, and deployment plan. In addition, the business sponsor must provide CBP with the camera's manufacturer information, including name, model, serial number, and firmware version. The TVS TRG contains specific requirements. Any required infrastructure and equipment must be procured and maintained by the business sponsor and/or its vendor. Upon the release of an updated version of the TRG, the business sponsor must provide a plan and a reasonable timetable to bring the solution back into compliance with any government-mandated changes. Any changes that are identified as "mandatory" must be implemented as soon as technically possible, but no later than 60 days. CBP may provide an extension upon request.	Upon review of the aforementioned documents (e.g., solution architecture), 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 FEDRAMP certification. All CBP requests for security documentation must be fulfilled and approved prior to "Go-Live" and connectivity with CBP's production environment. Existing partnerships will be required to comply within an agreed upon timeframe.

#	Requirement	Comments
4	The business sponsor and its systems integrator 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; (3) Berth; (4) Camera Model; and (5) Camera number. An example Device_ID is ATL-E-014-Vendor-01.	The TVS TRG mandates compliance with the Device_ID scheme on message elements. If the vendor recommends a different approach, CBP will consider all requests.
5	The business sponsor must provide the required power for use of TVS, as well as reliable and secure network access (e.g., high-speed internet and/or cellular).	The TVS TRG contains specific internet requirements. The business sponsor must provide CBP with the site's network/internet bandwidth no later than the activation of the solution.
6	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 signs in close proximity of and prior to the cameras, provide CBP-approved tear sheets, and facilitation of exemption processing for travelers who elect to opt-out). If e-signage is used, the CBP-approved language must be visible for the entirety of the boarding process. 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

#	Requirement	Comments
7	Any photos taken to facilitate TVS matching must not be stored and/or retained by the business sponsor or its systems integrator/vendor. All photos must be immediately purged from the business sponsor's system once a traveler has completed boarding. The business sponsor's system (including its systems integrator) must provide a mutually agreeable method by which CBP is able to audit compliance with this requirement.	An approved partner may collect photos of travelers using its own equipment under its own separate business process for its own commercial purposes. In this scenario, the business sponsor must distinguish its process from CBP's TVS enabled one through signage and other forms of public notice.
8	Any public communications regarding TVS 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, 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 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.
9	To ensure partners (cruise lines, port authority, etc) and staff understand the response from TVS, agent messaging must incorporate the three TVS response indicators: (1) No Match, (2) Recapture or Error/Issue, and (3) Match/Debark/Embark/Board. The three TVS related messaging responses above must be distinctly differentiated from non-TVS related messaging such as operational and technical messages including photo capture issues that result in no photo being sent to TVS. Color — Meaning Blue — No Match Yellow — Recapture or Error/ Issue Green — Match	It is important for cruise line staff to be able to identify different challenges. If a traveler is a no match, that will lead to one set of activities where poor image quality or facial capture issues will lead to different fixes. The business sponsor must work to ensure employees operating the system are trained to understand system messaging, ways to re-attempt photo capture when necessary, and how to approach and report technical problems. Additional messages should be included to help TVS end users (e.g., stakeholders, cruise line staff) clarify if issues are related to photo capture, traveler already boarded, software errors, and other non-TVS related issues, etc.

#	Requirement	Comments
10	Any TVS transactional data, to include unique IDs and matching results received from the original TVS response 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 a traveler has completed embarkation or debarkation. CBP partners should set retention and deletion time periods as cruise lines/ports may find it useful to have a few years of historical data such as match counts, retake rate, transaction counts, transaction time, etc. for comparison data over time. Any derived data that cannot be specifically tied to the original TVS response including match counts, hashed values of the UID, error counts performance time, etc., should not be considered under the retention and deletion parameters set by CBP.
11	For TVS performance standards, the TVS TRG contains requirements for system scalability, availability, and maintainability.	The TVS TRG states "Reliable, high-speed internet access is required. A hard-wired connection is preferred, but high-speed wireless will be adequate if the connection can be made reliable."
12	CBP must be allowed to review and/or assess any retained or derived data, code, encryptions, network connections and any other TVS related technical specifications.	

#	Requirement	Comments
13	The business sponsor must ensure that CBP-approved signage is posted at each location, while the biometric debarkation and embarkation is ongoing. The signage requirements are described below. The signage must be clearly visible and placed at a sufficient distance in front of the camera in order to provide the traveler with a reasonable opportunity to read the content and opt-out before reaching the photo capture area. Where signage is at least 22 inches wide and 28 inches tall, 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 (described below). Posted signage should never be smaller than 7 inches wide and 11 inches tall. Business sponsors can elect to display e-signage in either a static or slide show format. Should e-signage be displayed as part of a slide show, it must be visible for at least 45 seconds once every 5 minutes and be accompanied by at least one posted sign of a size no smaller than 7 inches wide by 11 inches tall. If the signage is displayed in a static format, it must be maintained as such throughout the entirety of the debarkation and embarkation process.	Signage will be reviewed periodically to ensure it is readable for travelers prior to photo capture to ensure all travelers have the ability to read and opt-out of the photo capture process. If a traveler chooses to opt-out, the traveler's identity must be manually verified against his/her travel document before permitting the traveler to board the vessel. Any updates to CBP mandated privacy signage must be posted as soon as possible (e.g., sufficient time for fabrication and posting). Business sponsors can find the most current version of communication materials on the CBP website. www.cbp.gov/biometrics
14	CBP will distribute TVS performance data to the business sponsor (and relevant biometric entry-exit program stakeholders) on an agreed-upon frequency that is operationally sustainable.	
15	CBP may require regular and ad hoc performance reporting on select systems integrated with TVS. Examples include but are not limited to: (a) estimated number of opt-outs; (b) camera capture rates; (c) number of travelers processed; (d) average photo quality scores; and (e) percentage of photos taken that were below the prescribed quality threshold.	

#	Requirement	Comments
16	Upon the identification of a system performance, security, or other issue, the business sponsor and its systems integrator must provide a detailed remediation plan and schedule. The business sponsor will provide progress reports to the CBP Biometric Entry-Exit Program Office on a mutually agreed-upon interval.	All remediation schedules must be completed as quickly as possible.
17	CBP must be notified of any cybersecurity-related incidents or breaches that occur on networks and hardware maintained by port authorities and cruise lines which are integrated with CBP's TVS. All known or suspected incidents or breaches shall be promptly reported to the CBP Biometric Entry-Exit 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.[3]	This requirement begins immediately once TVS integration is operational. Points of Contact: • Biometric entry-exit Program Office: Biometricsea@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)
18	The sponsor and/or vendor must ensure that all access to the software or hardware that is able to access TVS 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.	

[3] 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.

#	Requirement	Comments
19	The business sponsor's system must be designed to include a time-out mechanism for each camera when not in use for debarkation or embarkation operations.	The "time-out" feature should minimize any unintentional photographs taken of travelers that are not attempting to board the vessel.
20	Business sponsors are responsible for ensuring their participation in any TVS-related program is done in compliance with applicable federal and state laws and their relevant contracts. This includes any decision to integrate an e-gate into the biometric entry-exit solution. The business sponsor must confirm such equipment is compliant with applicable codes that govern relevant operations within their jurisdiction (e.g., fire code, the Americans with Disabilities Act, etc.)	
21	All maintenance of the equipment and software development provided by the business sponsor or relevant stakeholder in support of the TVS-related program is the responsibility of that business sponsor and/or the relevant participating stakeholders. Any personnel with access to equipment that is located on the vessel 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.	
22	The business sponsor and its systems integrator 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.

#	Requirement	Comments
23	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.
24	The business sponsor confirms that facial biometric debarkation and biometric sea entry-exit is a public-private partnership. Any requirement to conduct facial biometric debarkation and biometric sea entry-exit is between the traveler and the partnering cruise line.	While the public-private partnership is voluntary, CBP is Congressionally mandated to conduct biometric entry-exit.
25	TVS is allowed to be used for biometric entry-exit and only for CBP-approved TVS use cases.	If a partnering cruise line wishes to use TVS for an additional use case not specified, the written request must be submitted to CBP; and approved by CBP before activities begin.
26	Partnering cruise lines will identify the use cases where TVS is being used via the endpoint in the case of biometric sea entry-exit.	Approved partner TVS use cases are listed in requirement #25. Any partner misuse or use outside of those approved use cases (e.g., submitting queries for purposes that do not correspond to biometric sea entry-exit) will result in TVS access revocation and may be considered a breach as defined in requirement #17.

4. Operational Considerations and Recommendations

This section describes the operational considerations for partners conducting biometric entry-exit.

#	Operational/Onboarding Considerations	Comments
1	The business sponsor and its systems integrator must submit and receive approval for its deployment schedule.	
2	In the event that a traveler does not match through TVS, the partnering cruise line personnel (or its designee) at embarkation point must verify the traveler's identity against his/her travel document before permitting the traveler to board the vessel. If there is any concern about the authenticity of the travel document, or any concerns that the traveler is not the true bearer of the document, CBP can be contacted to adjudicate the matter. CBP will respond as soon as operationally possible. Operating under its own authorities and business processes, the cruise line can choose not to board the traveler if the traveler's identity is not adjudicated by CBP in time to allow for a timely departure.	The business sponsor and all relevant cruise lines must ensure that all personnel are trained on alternative manual processing for persons who do not match through TVS during processing.
3	It is highly recommended that all cruise line partners provide announcements that clearly convey the use of TVS and disclose the ability of travelers to opt-out of the process when cruise lines are conducting biometric entry-exit.	

#	Operational/Onboarding Considerations	Comments
4	The business sponsor must work with the relevant parties to ensure all vessel schedules, diversions, delays, and arrival/departure times are updated within the relevant systems as soon as possible.	If a vessel is significantly delayed without a corresponding update with a new departure time, biometric entry-exit processing/boarding may not be available.
5	If the business sponsor is a cruise line, then the cruise line must ensure that all identified APIS errors are corrected prior to departure/arrival to facilitate comprehensive gallery creation.	

Acknowledgement and Compliance Declaration

I, _____, acknowledge that I have received and read the Biometric Sea Entry-Exit Business Requirements Document (BRD) and Technical Reference Guide (TRG) on behalf of

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

Signature: _____

Name: _____

Title: _____

Date: _____

Appendix A: TVS Onboarding Guide

Upon commitment to implementing a biometric verification process, CBP will provide the business sponsor the TVS Technical Reference Guide(s).

New business sponsors/new vendor's solutions shall complete the following steps (in order) prior to using TVS in the production environment:

1. Review the TVS Technical Reference Guide(s);
2. Request access to the TVS in a Box (TIAB) environment using the TVS in a Box User Access Request Form;
3. Develop and test in the TIAB environment;
4. Request access to the TVS System Acceptance Test (SAT) and production environment using the External Vendor New CBP User Access Request Form;
5. Schedule and perform an integration test with the CBP TVS Team in the SAT environment;
6. Review and correct issues from the integration testing performed in the SAT environment; A joint "Go" or "No Go" decision shall be held with a planned outcome including revisions to the schedule as necessary; and
7. Upon completion of all testing activities, CBP will provide the TVS production environment user credentials. The business sponsor shall communicate to CBP of the planned production deployment date.

Steps 5-7 shall be completed if any of the following conditions are met:

- An existing business sponsor/vendor's solution is expanding to a new port.
    - Example: Cruise line ABC, the business sponsor, has an existing vendor's solution with vendor "X" at one port. ABC intends to expand biometric entry-exit to a new port with the existing vendor "X." This will require additional SAT testing with TVS.
- An existing business sponsor is using a new vendor solution.
    - Example: Cruise line ABC, the business sponsor, intends to add/use a new vendor. This will require additional SAT testing with TVS.
- An existing Business Sponsor/Vendor's Solution is expanding to a new cruise line.
    - Example: port authority XYZ, the business sponsor, has an existing solution with Cruise line "Gray." XYZ intends to expand and support cruise line "Blue" as well. This will require additional SAT testing with TVS.

The business sponsor/vendor's solution will also be required to provide a point of contact for password expiration notifications. This contact will receive notification when the business sponsor/vendor's solution password is about to expire. The TVS Team recommends providing a group mailing list in the event of any staffing changes.

Please send all completed forms to the CBP TVS Team using the email: tvssupport@cbp.dhs.gov.

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

CBP adheres to the following privacy principles when operating TVS:

- **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.[4]

[4] *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.