~~FOR OFFICIAL USE ONLY~~

U.S. Department of Homeland Security

U.S. Customs and Border Protection

Biometric Entry-Exit Program

Concept of Operations

April 20, 2017 June 27

Submitted by: (b) (6), (b) (7)(C)
Operational Sponsor, CBP, Office of Field Operations Date

Submitted thru: (b) (6), (b) (7)(C)
Program Manager, CBP, Office of Field Operations Date

Submitted thru: (b) (6), (b) (7)(C)
Director, CBP, Operational Requirements Branch Date

Endorsed by: (b) (6), (b) (7)(C)
Component Requirements Executive (CRE), CBP Date

Validated by: (b) (6), (b) (7)(C)
Director, DHS, Joint Requirements Council Date

* Endorsed by: (b) (6), (b) (7)(C)

* Note: See JRC Validation Memo dated 9/6/17 for specific CONOPs validation details.

~~FOR OFFICIAL USE ONLY~~

~~WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

Table of Contents

REVISION HISTORY V

PREFACE VI

EXECUTIVE SUMMARY 1

1 INTRODUCTION 3

1.1 Required Mission(s) and Need(s) 3
1.1.1 Threats 6
1.1.2 Strategy 9
1.1.3 Capabilities 10
1.2 MNS Capability Gap 11
1.3 Mission Operations Capability Description 12
1.3.1 Air 17
1.3.2 Land 18
1.3.3 Sea 19
1.3.4 Summary 19
1.4 Mission Support Capability Description 19
1.5 Mission Support Partners 20
1.6 Mission Support Community 21
1.6.1 Technical 23
1.6.2 Staffing 23
1.7 Current Situation 24

2 OPERATIONS AND SUPPORT DESCRIPTION 25

2.1 Missions (Primary/Secondary) 25
2.2 Users and Other Stakeholders 25
2.2.1 Users 25
2.2.2 Government Stakeholders 26
2.2.3 Non-Government Stakeholders 27
2.3 Policies, Assumptions and Constraints 27
2.3.1 Policy 27
2.3.2 Assumptions 28
2.3.3 Constraints 29
2.4 Operational Description 29
2.4.1 Air 30
2.4.1.1 Air Operating Concept 33
2.4.1.1.1 Air Departure 33
2.4.1.1.2 Air Arrival 33
2.4.1.2 Air Employment Modes 34
2.4.1.3 Air Scheduling and Operations Planning 34
2.4.1.4 Air Operating Environment 34
2.4.1.4.1 Geographic Areas 34
2.4.1.4.2 Environmental Conditions 34
2.4.1.4.3 Operational Conditions 34
2.4.2 Land 35

2.4.2.1 Land Operating Concept 35
2.4.2.2 Land Employment Modes 36
2.4.2.3 Land Scheduling and Operations Planning 36
2.4.2.4 Land Operating Environment 36
2.4.2.4.1 Geographic Areas 36
2.4.2.4.2 Environmental Conditions 36
2.4.2.4.3 Operational Conditions 36
2.4.3 Sea 37
2.4.3.1 Sea Operating Concept 37
2.4.3.2 Sea Employment Modes 37
2.4.3.3 Sea Scheduling and Operations Planning 37
2.4.3.4 Sea Operating Environment 37
2.4.3.4.1 Geographic Areas 37
2.4.3.4.2 Environmental Conditions 38
2.4.3.4.3 Operational Conditions 38
2.4.4 Threats and Hazards 38
2.4.5 Interoperability with Other Elements 38
2.5 Mission Support Description 39
2.5.1 Key Support Areas 39
2.5.2 Support Principles 42
2.5.3 Mission Support Concept 43
2.5.4 Mission Support Roles and Responsibilities 44
2.5.5 Mission Support Organization 45
2.6 Potential Impacts 46
3 SCENARIOS 48
3.1 Scenario Overview 48
3.2 Mission Operations Scenarios 48
3.2.1 Air Exit Pre-boarding Scenario (Optional) 48
3.2.1.1 Excursion 1 – Secondary Biometric Match (Optional Future Capability) 49
3.2.1.2 Excursion 2 – No Biometric Match 49
3.2.1.3 Excursion 3 – Watch List Hit 49
3.2.2 Air Exit Boarding Scenario 49
3.2.2.1 Excursion 1 – Facial Recognition No-Match 50
3.2.2.2 Excursion 2 – Watch List Hit 50
3.2.3 Land Pedestrian Exit Scenario 51
3.2.3.1 Excursion 1 – Facial Recognition No-Match 51
3.2.3.2 Excursion 2 – Watch List Hit 52
3.2.4 Land Vehicle Exit Scenario 52
3.2.4.1 Excursion 1 – Facial Recognition No-Match 53
3.2.4.2 Excursion 2 – Watch List Hit 53
3.2.5 Sea Exit Boarding Scenario 53
3.2.5.1 Excursion 1 – Facial Recognition No-Match 54
3.2.5.2 Excursion 2 – Watch List Hit 54
3.3 Mission Support Scenarios 55
3.3.1 Maintenance Support Scenario 58
4 FUNCTIONAL CAPABILITIES 59
4.1 Functional Capabilities Matrix 59

4.1.1 Mission Operations Matrix 59
4.1.2 Mission Support Matrix 60

5 CONOPS DEVELOPMENT TEAM 61

6 APPENDICES 62

6.1 ACRONYMS 62
6.2 REFERENCES 64

Revision History

Date	Section	Description
June 27, 2017	All	Initial Version

Preface

This Concept of Operations (CONOPS) describes the proposed Biometric Entry-Exit Program's operational and support capabilities that need to be developed to meet Customs and Border Protection (CBP) mission needs. In line with the Program's acquisition strategy, Acquisition Decision Event (ADE) 2A focuses on the development of the biometric matching capability, the Traveler Verification Service (TVS), which enables biometric identity verification and real-time queries against biometric databases for air, land, and sea travel modes. There will be separate ADE-2B milestones for each travel mode, which will further document how each will connect to the TVS. This CONOPS, along with other acquisition documentation will be updated to more clearly define the discrete operational capabilities that are unique to each travel mode as part of the preparation for each ADE-2B milestone.

A key driver for the development of a biometric entry-exit system is the Fiscal Year (FY) 2016 Consolidated Appropriations Act (P.L. 114-113), in which Congress established a biometric entry-exit fee that will provide up to $1 billion in funding over a 10-year period. A second key driver is Executive Order 13780, *"Protecting the Nation from Foreign Terrorist Entry Into the United States"* issued on March 6, 2017, which directs the Department of Homeland Security (DHS) to expedite the implementation of the biometric entry-exit system.

CBP is committed to leveraging DHS Enterprise Services where ever possible to meet the Biometric Entry-Exit Program mission and capability needs. CBP will leverage existing DHS enterprise biometric data repositories and will not create new ones. The biometric identity services provided by the DHS Office of Biometric Identity Management (OBIM) is a key resource for implementation of Biometric Entry-Exit Program capability. The Biometric Entry-Exit Program will utilize biometric data retained in OBIM Automated Biometric Identification System (IDENT) and its successor, Homeland Advanced Recognition Technology (HART), for biometrically confirming travelers crossing the border. CBP will not replicate data repositories for biometric data. Additionally, the Biometric Entry-Exit Program will provide biometric images captured at border crossings to OBIM IDENT/HART to build upon a traveler's encounter history in the DHS centralized enterprise biometric repository. CBP and OBIM are working collaboratively on a roadmap to define and achieve the end-state vision of maximizing the utilization of OBIM shared biometric matching service capabilities to support biometric confirmations of all air, land, and sea travelers. While the roadmap is executed, CBP will in parallel implement a biometric matching capability meeting the operational requirements necessary to biometrically confirm travelers at border crossings without impacting the flow of travel and deployed in an expedited manner as directed by EO 13780.

Executive Summary

This Biometric Entry-Exit Program CONOPS describes the operational and support capabilities required to meet CBP's mission needs. The primary mission of CBP is to safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling lawful international trade and travel. A key aspect of this mission is the ability to discern travelers' admissibility into the United States (U.S.) and validate travelers' departure in compliance with terms of admission. The Biometric Entry-Exit Program will fuse biographic and biometric data and technology to improve verification of identities for all travelers entering and exiting the U.S.

The Program's Capability Analysis Report (CAR) and Mission Need Statement (MNS) identified several needed capabilities to enhance CBP's ability to execute its border security mission:

- **Verify Traveler Identity** – The ability to capture, review, analyze, search, and match an in-scope[1] traveler's biometric information against biometric and biographic records when entering and exiting the U.S. for the purposes of verifying identity.
- **Create and Manage Biometric Records** – The ability to record, store and disseminate biometric information and metadata collected from in-scope, non-U.S. citizen travelers entering and exiting the U.S. CBP will leverage DHS Enterprise Service capabilities for biometric repositories.
- **Generate Metrics and Reports** – The ability to measure and report the effectiveness of the biometric entry-exit system.

Based on CBP's operations and the evaluation of a number of biometric field trials conducted at air, land, and sea ports of entry (POE), CBP has identified the following mission needs required to successfully implement a biometric entry-exit approach:

- **Develop Biometric Entry and Exit Operations Policy** – Comprehensive traveler entry and exit policies and procedures governing the use of biometric data to determine legal ability to enter and exit the U.S.
- **Establish Biometric System Access Authorities** – The authorities and pre-approved permissions to access, request, search, discover, and retrieve biometric data.
- **Utilize Existing Entry and Exit Inspection Areas** – Points of departure and entry control at each POE.
- **Utilize Existing Entry-Exit Physical Infrastructure** – Physical facilities and infrastructure to support entry and exit control operations at each POE.

[1] Includes all travelers, U.S. and non-U.S. citizens, between the ages of 14 and 79.

- **Build-Out Information Technology Infrastructure** – Information technology (IT) infrastructure to digitally connect CBP POE entry–exit control sites to external law enforcement and biometric databases.

For exit, the air environment is CBP's top priority with land and sea to follow. Biometric exit solutions developed for air will be leveraged as much as possible for land and sea. Entry solutions and technical upgrades will be introduced to support exit. Under its Biometric Pathway Vision of using biometrics as the key to enhancing security and unlocking benefits, CBP is working in partnership with the air travel industry to lead the transformation of air travel which will dramatically improve the entire traveler experience. Biometrics will be used to streamline and secure passenger processes throughout the air travel continuum as well as provide airport and airline entities with a frictionless method to utilize validated information from DHS systems.

To achieve the Biometric Pathway Vision, CBP will implement a biometric matching capability called the Traveler Verification Service (TVS) to be used by travel industry stakeholders or by CBP itself to identify travelers throughout the travel process. TVS is defined as a robust, advanced, integrated, technical service to support advanced identity verification and real-time queries against databases that pre-position traveler information utilizing cloud architectures. TVS capability will leverage existing government holdings (such as OBIM IDENT/HART and Department of State) to create small, targeted biometric galleries of expected travelers based upon travel manifest data. TVS will align with the Homeland Security Enterprise Architecture (HLS EA) through the CBP Architecture, Alignment and Assessment (AAA) process and the DHS Enterprise Architecture Board (EAB) governance process, as applicable. TVS will leverage DHS Enterprise Services capabilities where possible to meet its mission needs. CBP and OBIM will create a roadmap for integrating biometric matching services from OBIM. The solution will incorporate an automated means of generating hotlists[2] based upon actionable biometric and biographic watch list hits and identification of aliens who may have entered the U.S. without inspection. A Passenger Analysis Unit (PAU) validates hotlists and the need for CBP to talk to a traveler. CBP Officers (CBPO) will receive mobile notifications when a traveler is identified with a hotlist hit. Biometrically confirmed border crossings will be recorded for in-scope, non-U.S. citizen travelers in OBIM IDENT/HART, TECS, and the Arrival Departure Information System (ADIS).

Mission support is essential to the successful implementation of the Biometric Entry-Exit Program. To achieve this, the Program has adopted a Mission Support Business Model (MSBM) that provides a mission-focused, unified, and disciplined approach to mission support delivery.

[2] A hotlist refers to an automated list of travelers validated by a PAU who CBP has a need to talk to when encountered during border crossing.

CBP has established a Program Management Office (PMO) within the Office of Field Operations (OFO) to manage the Biometric Entry-Exit Program and to apply the MSBM.

The system security, confidentiality, integrity, and availability are of upmost importance for meeting the Biometric Entry-Exit Program mission. The system will comply with CBP and DHS security policies and associated guidance to include DHS Sensitive System Policy Directive 4300A and NIST 800-53 Rev 4 (or any future versions) Security and Privacy Controls for Federal Information Systems and Organizations.

The solution will ensure privacy and compliance with DHS Management Directive (MD) 047-01, Privacy Policy and Compliance and all applicable privacy policies, procedures, instructions, and internal controls necessary to safeguard personally identifiable information (PII) pursuant to the Privacy Act, as well as compliance with the Department's guidance for accommodating religious beliefs in DHS policies requiring fingerprinting or photographic identification and disability accommodations.

1 Introduction

1.1 Required Mission and Need

The National Commission on Terrorist Attacks Upon the United States (a.k.a. 9/11 Commission) final report identified capability gaps related to traveler identification and highlighted the need for a biometric entry-exit system as an "essential investment in our national security." DHS has invested resources in improving or creating systems that rapidly and efficiently share data that enhances CBP's mission effectiveness while minimizing negative impacts on lawful travel. These changes make it possible to further enhance the traveler entry and exit biometric capability to comply with federal law.

The primary mission of CBP is to safeguard America's borders from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel. CBP has the ongoing mission to inspect all incoming people, goods and conveyances to determine admissibility to the U.S. and enforce and administer U.S. immigration and customs laws. Every day CBP processes over 1 million travelers as they enter the U.S. at air, land, and sea POEs. By comparison, over 1 million travelers also depart the U.S. daily with approximately 700,000 departing at a land border, 300,000 by an airplane, and 50,000 by a sea vessel. CBP operations in the exit environment is limited to identifying and detaining individuals subject to a law enforcement action or through random inspection of people as they board an airplane, vessel, or cross a land border.

Under existing laws and Executive Order 13780[3], CBP is required to implement measures that will enable CBP to verify the identities of all travelers at entry to and exit from the U.S., including U.S. citizens, through the fusion of biographic and biometric data and technology. Biographic data includes information specific to an individual traveler including name, date of birth, and travel document number and is stored in that traveler's passport, visa, lawful permanent travel card, or other authorized travel document. Biometric data includes information captured from fingerprints, facial images, or other characteristics that are unique to an individual. Biometric data, when used with biographic data, allows CBP to confirm with greater assurance a traveler's true identity, match to previous encounters with CBP and other government entities, and conduct biometric watch list checks. As biometric technology has evolved, the ability to use individual characteristics to confirm identity for all travelers, including U.S. citizens, is now a reality for all modes of transportation.

To understand the breadth of the required capability needs to meet this challenge, CBP prepared the Biometric Entry-Exit CAR, which identified those operational capabilities that will need to be developed to meet the challenge of verifying the identities of all travelers through the fusion of biographic and biometric data. These operational capability needs will comply with the DHS Enterprise Architecture to facilitate secure data sharing between existing systems, thereby enhancing traveler identify and screening processes.

CBP has identified several needed capabilities to enhance the ability to identify travelers including:

- **Verify Traveler Identity** – The ability to capture, review, analyze, search, and match an in-scope[4] traveler's biometric information against biometric and biographic records when entering and exiting the U.S. for the purposes of verifying identity.
- **Create and Manage Biometric Records** – The ability to record, store and disseminate biometric information and metadata collected from in-scope, non-U.S. citizen travelers entering and exiting the U.S. CBP will leverage DHS Enterprise Service capabilities for biometric repositories.
- **Generate Metrics and Reports** – The ability to measure and report the effectiveness of the biometric entry-exit system.

Based on CBP's operations and the evaluation of a number of biometric field trials conducted at air, land, and sea POEs, CBP has identified the following mission needs required to successfully implement a biometric entry-exit approach:

[3] https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreign-terrorist-entry-into-the-united-states

[4] Includes all travelers, U.S. and non-U.S. citizens, between the ages of 14 and 79.

- **Develop Biometric Entry and Exit Operations Policy** – Comprehensive traveler entry and exit policies and procedures governing the use of biometric data to determine legal ability to enter and exit the U.S.
- **Establish Biometric System Access Authorities** – The authorities and pre-approved permissions to access, request, search, discover, and retrieve biometric data.
- **Utilize Existing Entry and Exit Inspection Areas** – Points of departure and entry control at each POE.
- **Utilize Existing Entry-Exit Physical Infrastructure** – Physical facilities and infrastructure to support entry and exit control operations at each POE.
- **Build-Out Information Technology Infrastructure** – IT infrastructure to digitally connect CBP POE entry–exit control sites to external law enforcement and biometric databases.

CBP has been actively examining joint requirements for biometric capabilities across DHS since the inception of the Joint Requirements Council (JRC) and has led several initiatives to improve cross-component collaboration. Along with other DHS components, CBP helped to develop a DHS-wide *Biometrics Strategic Framework*[5] in 2015 and in 2016 the *Biometrics Roadmap Winter Study*[6] to guide biometric implementations across the department.

CBP performed a number of biometric field trials which identified a series of mission needs that have been aligned to DHS mission areas. Table 1, Alignment to DHS Mission Areas, summarizes the biometric entry/exit mission need alignment to DHS mission areas as identified in the *2014 Quadrennial Homeland Security Review*[7].

Table 1 – Alignment to DHS Mission Areas

		DHS MISSION AREAS			
		PREVENT TERRORISM AND ENHANCE SECURITY	SECURE AND MANAGE OUR BORDERS	ENFORCE AND ADMINISTER IMMIGRATION LAWS	SAFEGUARD AND SECURE CYBERSPACE
BIOMETRIC ENTRY/EXIT MISSION NEEDS	OPERATIONS POLICY	X	X	X	
	BIOMETRIC SYSTEM ACCESS AUTHORITIES				X
	ENTRY/EXIT INSPECTION AREAS	X	X	X	
	PHYSICAL INFRASTRUCTURE		X		
	IT INFRASTRUCTURE		X		X

[5] https://www.hsdl.org/?view&did=786880

[6] http://dhsconnect.dhs.gov/org/comp/plcy/spar/Winter%20Studies/Biometrics%20Roadmap%20Winter%20Study_Final%20Report_April%2015%202016.pdf

[7] https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

Table 2, Alignment to CBP Mission Areas, summarizes these five biometric entry/exit mission needs and aligns them to CBP mission areas outlined in the *CBP Vision and Strategy 2020*[8]. This assessment is based on current CBP operations and findings from biometric field trials.

Table 2 – Alignment to CBP Mission Areas

		CBP MISSION AREAS			
		COUNTER TERRORISM AND TRANSNATIONAL CRIME	ADVANCE COMPREHENSIVE BORDER SECURITY AND MANAGEMENT	ENABLING LAWFUL TRADE AND TRAVEL	PROMOTE ORGANIZATION, INTEGRATION, INNOVATION, AND AGILITY
BIOMETRIC ENTRY/EXIT MISSION NEEDS	OPERATIONS POLICY	X	X	X	X
	BIOMETRIC SYSTEM ACCESS AUTHORITIES		X		X
	ENTRY/EXIT INSPECTION AREAS	X	X	X	
	PHYSICAL INFRASTRUCTURE		X	X	
	IT INFRASTRUCTURE			X	X

1.1.1 Threats

Threats in CBP's ability to execute its border security mission exist on multiple levels:

- **Threats to the Public** – Public safety is paramount. The threat of terrorism in an uncontrolled or uncontrollable environment significantly raises the risk of harm or injury to the traveling public. This can include threats to the security of PII which can create identity management issues for impacted individuals.
- **Threats to CBP Operations** – The disruption of CBP operations may cause minimal to significant delays (for example, flight delays) depending on the severity of the threat. The resulting increased processing times would seriously affect CBP's mission to secure and facilitate lawful travel. The inability to secure PII threatens CBP's ability to perform reliable biometric matching and increases the probability of CBP allowing individuals traveling under a false or assumed identity to enter and/or exit the U.S.
- **Threats to Technology** – The inability to access, receive, and secure necessary identity information on travelers will significantly impact CBP's ability to facilitate lawful travel. This also increases the threat to data integrity, which increases the probability of allowing individuals to enter and/or exit the U.S. under a false of assumed identity.

Table 3 describes the threats, impacts, and the avoidance objectives.

[8] https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf

Table 3 - Threats, Impact and Avoidance Objectives

Threat Description	Threat Impact	Threat Avoidance Objectives
Inability to Accurately Verify Identity at Entry and Exit – The inability to accurately verify the identity of a person entering or exiting the country may allow terrorists or other people of interest or known criminal behavior to enter or remove themselves from the country and continue nefarious activities. These activities may result in injury or death to many people as well as destruction of public or private property and destruction of sensitive data through cyber terrorism or espionage.	• Public • Operations • Technical	• Prevent, avoid, or stop an imminent, high risk traveler from performing an actual act of terrorism. • Enhance CBP enforcement policies and operational business processes to remain agile and adaptable in supporting operational requirements to ensure efficiency and effectiveness. • Systemically respond in a timely manner to identify the level of suspected threat of inbound and outbound travelers, protect property and the environment, and prevent acts of terrorism. • Deploy an advanced, integrated, secure technical infrastructure to support advanced identity verification and real-time queries against databases that pre-positions traveler information which will allow CBP Officers to assess quickly, reliably and accurately traveler information prior to exiting the country. • Redesign or reconfigure physical areas and/or operational procedures to support secure processing of detained travelers.
Ensure Departure from the U.S. – The inability to ensure that a traveler has physically departed the country may result in people staying in country who have overstayed the visa or authorized period of admission, thus being in violation of immigration laws.	• Public • Operations • Technical	• Systemically respond in a timely manner to identify the level of suspected threat of outbound travelers, protect property and the environment, and prevent acts of terrorism. • Processing and translating data into meaningful information to determine a suspected traveler's threat level. • Deploy an advanced, integrated, secure technical infrastructure to support advanced identity verification and real-time queries against databases that pre-positions

Threat Description	Threat Impact	Threat Avoidance Objectives
		traveler information which will allow CBP Officers to assess quickly, reliably and accurately traveler information prior to exiting the country.
Ensure Protection of Personal Data – Centralized storage and regular transmission of sensitive, personal data impacts the confidentiality, integrity, and availability of biometric PII data which may increase the risk of identity theft and other harm to individuals.	• Public • Technical	• Processing and translating data into meaningful information to determine a suspected traveler's threat level Processing and translating data into meaningful information to determine a suspected traveler's threat level. • Comply with CBP's Enterprise Technology Architecture (ETA) guidance. • Comply with DHS and CBP information system (IS) security and technology policy. • Ensure use of strong end-to-end encryption of all data. • Verify information requests to avoid compromise, exfiltration, and exploitation of derogatory information held by the government by an individual or organization seeking to subvert the entry and exit process. • Regularly test systems for vulnerabilities by external and internal threats including auditing of user logs. • Protect and properly label information that may be shared that is classified under 8 U.S.C. § 1367 and 8 CFR 208.6

The Biometric Entry-Exit Program will help mitigate the threats of not being able to accurately verify identity and ensure departure of travelers by providing the following benefits:

- Enhance identity assurance by collecting biometrics at U.S. departure.
- Use of biometrics to match arrival and departure records.
- Help identify travelers who are traveling using fraudulent documents and identify imposters traveling with genuine documents.

- Provide the capability to search biometric watch lists with live biometrics captured during border crossings.

1.1.2 Strategy

The strategy for implementing a successful biometric entry-exit solution that is both feasible and realistic will include a high scalability factor based on the key parameters and considerations identified in Table 4.

Table 4 – Key Strategic Parameters

Key Strategic Parameter	Description
Do not add another processing layer to known travel processes.	Avoid a stove piped, independent approach by integrating biometrics into already existing travel processes.
Utilize existing infrastructure	The solution will work in existing port infrastructure for entry and exit processing.
Utilize existing business models	Leverage existing stakeholder (airline, cruise line) systems, processes and business models.
Leverage Current Passenger Behavior	Leverage passenger behaviors and expectations that require minimal new or unexpected steps for travelers.
Leverage Existing Data & IT Infrastructure	Leverage existing traveler data such as IDENT, Advance Passenger Information System (APIS), Automated Targeting System (ATS), TECS, Arrival and Departure Information System (ADIS), etc. and leverage existing government IT infrastructure as much as possible.
Utilize existing DHS enterprise biometric matching services, capabilities, and investments	Leverage and integrate with DHS Enterprise Services for shared biometric matching capabilities following the CBP and OBIM Integration roadmap.

For the initial implementation of biometric exit solutions in the air environment, CBP will work in partnership with the air travel industry to lead the transformation of air travel using biometrics as the key to enhancing security and unlocking benefits, which will dramatically improve the entire traveler experience. CBP's transformative Biometric Pathway vision will realize the benefits identified in Table 5.

Table 5 - Strategic Benefits

Strategic Benefit	Description
Improved Business Process	An enhanced Entry-Exit business process that integrates within existing government and stakeholder business models.
Stronger Relationships	An environment that allows CBP and stakeholders to work together and that allows for further airline modernization.
Enhanced Security	An overall enhanced and seamless traveler experience.
Improved Traveler Experience	An overall enhanced and seamless traveler experience.

Strategic Benefit	Description
Improved Data Integrity	Utilize DHS enterprise biometric repositories provided by OBIM to ensure accurate biometric identity records.
Enhanced Visa Overstay Enforcement	Support the identification and tracking of visa overstays by closing information gaps associated with current exit reporting capabilities allowing for improved enforcement action.

For air travel, CBP will utilize the biographic Advance Passenger Information System (APIS) manifest data and existing photographic images of travelers (United States Citizens (USCs) and non-USCs) already in government databases such as IDENT to build small targeted biometric galleries. These galleries will be searched with live photographic images taken at departure to determine the identity of the traveler in order to biometrically confirm the exit. CBP will provide a Traveler Verification Service for use by stakeholders (such as airlines, airports, Transportation Security Administration (TSA), or CBP itself) who will deploy front end biometric capture devices and securely submit live biometric images for matching. The biometric matching capabilities will leverage DHS Enterprise Services in accordance with the CBP and OBIM integration roadmap.

Biometric exit solutions for land and sea travel will leverage appropriate solutions developed for air and follow consistent strategies. Commercial sea travel is similar to commercial air travel in that travel manifest information is provided to CBP. Additionally, sea carriers may already capture photographs of passengers for their own processes or could integrate photo capture on embarkation and debarkation. For land, it is envisioned frequent crossing populations will be able to benefit from building small localized galleries to match against.

1.1.3 Capabilities

To efficiently implement a biometric entry-exit approach and to aid in mitigating threats listed in Table 3, the following CBP operational capabilities will be enhanced or developed:

- **Verify Traveler Identity**
  - Biometrically confirm the identity of all U.S. citizen and non-U.S. citizen travelers between the ages of 14 and 79. To prevent the need to segment travelers or other operational challenges, U.S. citizens and non-U.S. citizens' identities will be biometrically confirmed upon exit. However, once U.S. citizenship of a traveler is confirmed, that traveler will not be further processed and the live image will not be retained.
  - Utilize existing government biometric holdings (photos and fingerprints) to compare to live images captured at border crossing.
  - Provide mobile alerts to CBP Officers when a biometric match is not made; match is made to an identity with actionable biometric or biographic watch list hits, or the traveler is determined to be a person who originally entered the U.S. without inspection.

- **Create and Manage Biometric Records**
  - Provide biometric exit transactions for in-scope, non-U.S. citizen travelers to OBIM IDENT/HART for biometric verification and exit recording.
  - Provide biometric exit confirmation for in-scope, non-U.S. citizen travelers in TECS and ADIS.
- **Generate Metrics and Reports**
  - Provide the capability to view biometric match results localized for a specific port, gate, or flight and also in aggregate.
  - Provide the capability to view biometric match results by traveler demographics.
  - Provide the capability to view response time performance of the biometric matching system.
  - Provide the capability to view performance metrics for time to build galleries to include time from receiving APIS transmissions to the time the photo is included in the gallery.
  - Monitor the performance of external biometric capture devices by collecting descriptive data that informs the type of capture device, the type of image, etc.

1.2 MNS Capability Gap

Today, CBP has a wide range of capabilities to support CBP's mission to determine a traveler's legal ability to enter and exit the U.S. In assessing these capabilities, CBP has identified a number of areas where current capabilities will be insufficient or incapable of meeting the mission need to biometrically verify the identity of travelers upon entry to or exit from the U.S.

Based on this assessment, CBP has insufficient biometric regulations and policies to fully conduct biometric entry and exit operations at POEs. While CBP currently leverages existing physical facilities and infrastructure, these POEs also uniformly lack sufficient entry-exit inspection areas and associated physical facilities and infrastructure required to support and record the entry to and exit from the U.S. for all in-scope, non-U.S. citizen travelers. CBP lacks the required IT infrastructure to process large volumes of biometric data from departing travelers and for CBP to take action when required. CBP also lacks the ability to access, request, review, analyze, search, match, and identify 100% of travelers exiting the U.S. CBP has insufficient capabilities to measure and report the effectiveness of a comprehensive biometric entry-exit system.

Currently, there is no one single solution that can fill these capability gaps. CBP has been engaged in a number of biometric field trials that were established to evaluate the ability to capture a biometric identifier and validate a traveler's identity. For example, some of these field trials have included field testing of CBP's ability to compare a live capture facial image with the traveler's passport photo at airports. Another field trial at a land POE evaluated the ability

to capture a person's iris and face at entry for comparison when that traveler exited from the U.S. Based on this experience, CBP is prepared to begin identifying solutions that will address each identified capability gap. To enable CBP to further define potential solutions, Table 6 summarizes the identified capability gaps aligned to the Doctrine, Organizations, Training, Materiel, Leadership, Personnel, and Facilities, plus Regulations/Grants/Standards (DOTmLPF-R/G/S) framework.

Table 6 – Capability Gaps

Capability Gaps	DOTmLPF-R/G/S Factors									
	D	O	T	m	L	P	F	R	G	S
Verify Traveler Identity	X		X	X		X	X	X		
Create and Manage Biometric Records	X			X				X		
Generate Metrics and Reports				X						

1.3 Mission Operations Capability Description

Mission operations capabilities are uniquely defined for air, land and sea travel. Air is CBP's first priority closely followed by land and sea. Capabilities developed for air will be leveraged for land and sea to the greatest extent possible while also meeting the unique capability needs for each mode of travel.

Figure 1, Biometric Entry-Exit Program Use Cases, provides a high-level view of the systems, users, operators, external entities and their interrelationships. The diagram provides the functional capability mapping with system users and other external entities. The high-level use cases represent the functional capability of the system and the actors represent the users and external entities that interact with the system. The overall concept of operations is to implement a traveler verification service (TVS) to be utilized for all modes of travel – air, land and sea. The matching capabilities may be deployed in a cloud environment for scaling and performance considerations. TVS will align with the Homeland Security Enterprise Architecture (HLS EA) through the CBP Architecture, Alignment and Assessment (AAA) process and the DHS Enterprise Architecture Board (EAB) governance process, as applicable. CBP is committed to working with DHS OBIM to realize a common, enterprise-scale, shared biometric matching service in support of CBP's biometric entry-exit operations. Front-end biometric capture devices will be implemented at all ports either by commercial travel partners (which is the preferred approach for air and sea) or by CBP itself (for land) to capture and securely submit live biometric images for matching. The system will adapt to the unique requirements for air, land, and sea.

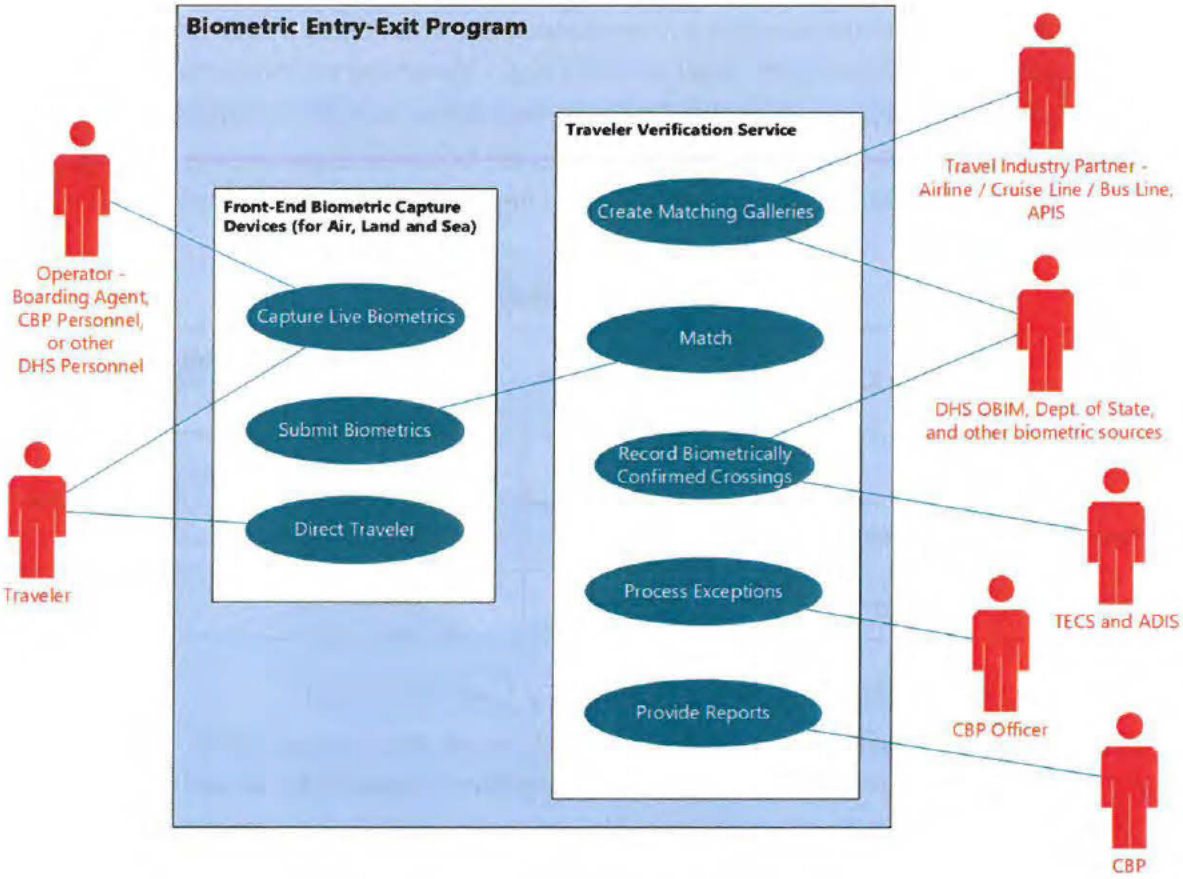


Figure 1 - Biometric Entry-Exit Program Use Cases

System Actors

Table 7 describes the external entities who will interact with the Biometric Entry-Exit Program.

Table 7 – System Actors

System Actors	Description
Operator	An operator of a front-end biometric capture device located in air, land, and sea port of entries assists travelers with the capture of biometrics and helps direct travelers to proceed, recapture biometrics, or wait for further assistance based upon the response received from TVS. In the scenario where air and sea travel industry partners integrate front-end biometric capture devices into their boarding operations, the operators are employees of those private companies. At land ports and in the instances where CBP operates front-end capture devices at air and sea ports, the operators are CBP personnel. Other DHS components such as TSA or ICE may implement and operate front-end biometric capture devices. An operator may provide

System Actors	Description
	active or passive assistance to travelers. In the case of self-service front-end capture devices, an operator may just monitor travelers and provide support for exceptions. An operator does not perform law enforcement actions. Only CBP Officers will conduct law enforcement operations.
Traveler	A member of the public entering and exiting the country. This includes commercial, crew, and private travelers in all modes of travel (air, land, and sea), both USC and non-USCs.
CBP Officer	A CBP Officer receives notifications and responds to travelers identified with actionable biometric watch list hits and to travelers that likely entered the country without an inspection. A CBP Officer will perform all activities that they are engaged in today via current Standard Operating Procedures (SOPs) and policies however with the benefit of additional information received from the Biometric Entry-Exit Program.
Travel Industry Partner, APIS	Consist of commercial airlines, cruise lines and bus lines that securely submit passenger manifest data to CBP prior to travel via APIS. Also consists of commercial airlines, airports, and cruise lines who implement front-end biometric capture devices into their boarding processes for passengers exiting the country. Travel industry partners may also include other government stakeholders such as the TSA who implement front-end biometric capture devices to utilize TVS.
DHS OBIM and other Biometric Data Sources	DHS OBIM is the primary source of biometric data utilized for matching. CBP also utilizes other government biometric data sources Including the following: • Department of State (DoS) for U.S. Passports • Non-U.S. passport (ePassport from previous Entry) • Automated Passport Control (APC) • Consular Electronic Application Center (CEAC) • Central Index System (CIS) • Global Enrollment System (GES) • VISA • Enforcement Integrated Database (EID) Biometric sources may change over time to insure CBP has access to the images necessary to build galleries that can be used to successfully biometrically match travelers.

System Actors	Description
	DHS OBIM will contain biometrically confirmed crossing records. OBIM will provide matching services according to the CBP and OBIM Integration Roadmap.
TECS and ADIS	TECS and ADIS will contain indicators of biometrically confirmed crossings for in-scope, non-U.S. citizen travelers.

System Use Cases

Table 8 describes how the actors will interact with the Biometric Entry-Exit system in order to achieve the mission.

Table 8 – System Use Cases

Use Case	Description
Front-End Biometric Capture Device Functions	
Capture Live Biometrics	A traveler will interact with front-end biometric capture devices to collect live biometric images during border crossings. An operator may assist the traveler with the biometric capture.
Submit Biometrics	The front-end capture devices will securely submit live biometric images to and receive responses from TVS.
Direct Traveler	The front-end capture devices will direct a traveler to proceed, recapture biometrics, or wait for additional processing based upon the response received from TVS.
Traveler Verification Service	
Create Matching Galleries	TVS will receive passenger manifest data from travel industry partners such as commercial airlines, cruise lines, and bus lines to develop logical or physical galleries to support real time matching of travelers at border crossings.
Match	TVS will receive live biometric images from front-end biometric capture devices and search the appropriate targeted matching gallery. A match or no match response is returned to the front-end biometric capture device. The operator, traveler, and CBP Officer (for exception cases) receive match results.
Biometrically Confirm Crossing	In the event of a biometric match, a biometrically confirmed crossing is recorded for in-scope, non-U.S. citizen travelers in DHS OBIM and indicated in TECS and ADIS. In the event that CBP and OBIM's determination of a biometric match are different, a reconciliation process will be required.
Process Exception	In the event of a biometric match occurring for travelers identified with actionable watch list hits and probable entry

Use Case	Description
	without inspections (EWIs)[9], the service will notify CBP Officers and provide the information necessary for responding. Additionally, if a traveler fails to match to a record in the gallery, CBP Officers will be notified. CBP Officers will respond to notifications based upon outbound policy.
Provide Reports	TVS will provide reporting data to authorized CBP personnel that will provide gallery details, match results, and exception data. The reporting capability will provide overall and segmented views of the data. Segmentation will include parameters such as port of entry, airport, terminal, gate, flight, airline, citizenship, and traveler demographics,

Mission Partners

Mission partners include other government agencies as well as the commercial travel industry. DHS OBIM is the prime repository of traveler biometric data that will be utilized for biometrically confirming border crossings. U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), TSA, Department of State, and other Federal and State agencies will participate in data sharing and, where applicable, law enforcement activities in support of mutual mission needs, pursuant to an approved information sharing agreement. The commercial travel industry such as airlines, airports, cruise lines, and bus lines will adapt their operations to either collect biometrics or support CBP collecting biometrics of passengers at border crossings. See section 2.2, Users and Other Stakeholders, for further description of the roles of government and non-government mission partners.

Mission Operations Community

The mission operations community includes operators who assist travelers with collecting biometrics as well as CBP Officers who respond to travelers when required. The concept of operations for air and sea is for travel industry partners to capture live biometrics with their own devices following CBP specifications and securely submit to CBP for matching. In this instance, the travel industry staff that assists passengers with the collection of biometrics become part of the mission operations community. For land and instances where air and sea travel industry partners are not collecting live biometrics, CBP Officers will assist travelers as necessary. Additionally, for all modes of travel, CBP Officers will respond as required to travelers identified with actionable watch list hits and probable EWIs and to travelers who cannot be biometrically confirmed.

[9] A Probable Entry Without Inspection (EWI) is a traveler that is likely to have entered the United States through a means other than an official port of entry. A probable EWI has no official record of arrival with CBP.

1.3.1 Air

For commercial air travel, CBP envisions an end-state where biometrics streamline the passenger process; from passenger arrival at the airport; through TSA processing, and international arrival and/or departure. Through partnerships with airlines, airports and TSA, CBP can deliver an integrated biometric exit solution that provides significant benefits to the participating partners in addition to meeting the congressional mandate for a biometric exit system.

All participants in the travel continuum, (airlines, airports, TSA, and CBP) are facing fixed airport infrastructure with little opportunities for major investment, increased national security threats with pressures for solutions, and increased traveler volume. Collectively, this is a status quo that is not sustainable for any of the main stakeholders, and failure to change will ultimately result in increases in dissatisfied customers, use of alternative modes of travel, and vulnerability to serious threats.

Creating a biometric air exit system independent of the other pieces of the travel continuum is a missed opportunity to transform the overall traveler experience. By partnering with other stakeholders, CBP can facilitate a large-scale transformation of air travel that, by using biometrics, will make air travel more:

1) secure, by providing increased certainty as to the identity of airlines travelers at multiple points in the travel process,
2) convenient and easier for individual travelers, by eliminating the need for multiple document and boarding pass checks,
3) predictable, by establishing a clear and easily understood process that will reduce the potential for major "bottlenecks" within the air travel process, and
4) able to build additional integrity to the immigration system, by better identifying which foreign nationals are violating the terms of admission to the United States, and by providing capability for immediate action when that occurs.

This vision will deliver benefits to CBP, TSA, the airlines, the airports, and the traveling public by simultaneously delivering additional security while streamlining existing processes. Expansion of biometric capabilities is uniquely able to deliver on both points. Instead of a program that is built and developed exclusively by CBP, and that benefits only CBP missions, the result is a series of inter-connected initiatives undertaken by multiple stakeholders, both public and private, and through which all will significantly benefit.

General aviation (GA) includes all civil aviation operations other than scheduled air services and non-scheduled air transport operations for remuneration or hire. Any airplane arriving from a foreign country or foreign soil is subject to the same rules and regulations for immigration that apply to commercial air travel. The dynamic nature of general aviation makes it much more

difficult to manage and control in terms of achieving the critical mission objective; specifically ensuring the identity of all travelers leaving the country. Traveler manifest data for general aviation can be leveraged to follow the same concept as commercial aviation. Additionally, general aviation may include a self-reporting approach implemented and integrated into the overall system.

1.3.2 Land

The CBP land border entry and exit capability supports the following modes of travel along the Southern and Northern borders:

- Privately Owned Vehicles (POVs)
- Commercial Buses
- Pedestrian
- Ferries
- Rail

Each mode of land travel requires unique capabilities to address operational and environmental conditions to perform biometric confirmations while not impacting passenger and commercial traffic for arrivals and departures. Additionally, since land travel is mostly unscheduled, CBP does not have the benefit of receiving passenger manifest information prior to travel as it does with air and sea. Because most arrivals at land ports are unscheduled, a person's identity and citizenship cannot be verified using presented documentation until arrival at the primary inspection point. Proper inspection processing without advanced traveler information can take a considerable amount of time and result in severe congestion during peak crossing times at busy ports. In POV lanes, CBP requirements (such as the capability to photograph travelers who are still inside vehicles) are not compatible enough with air requirements to simply apply the air solution to land. Additionally, CBP is the owner of primary vehicle lanes (unlike the air environment, where a departure gate is owned by an airport authority or airline). This means responsibility for owning and operating the front-end capture devices will fall to CBP. Travelers arriving by bus or on foot interact with CBP Officers in essentially the same manner as do air travelers; therefore, the solution in the air environment will have greater applicability.

Travelers departing the United States generally leave utilizing the same mode of travel they came; however, CBP land border facilities, like airports are not designed to facilitate exit processing. The first priority for land exit is to biometrically confirm the exit of third country nationals (TCNs). CBP will utilize existing systems and resources to the greatest extent possible to biometrically confirm exit of TCNs. In the longer term, CBP planning will focus primarily on holding travelers accountable for self-reporting departure with a biometric verification component. If a traveler does not self-report the departure, CBP will assume the traveler is still in the United States (meaning the traveler would violate the terms of admission and not be

eligible for re-admission). CBP will simultaneously continue to test advances in biometric technologies for application in land ports. Additionally, CBP planning will focus on a data exchange with Mexico and Canada (an entry into Mexico or Canada assumes an exit from the United States) and encourage biometric sharing.

1.3.3 Sea

Because of the similarities between U.S. seaports and aviation ports for commercial travel, CBP plans to leverage solutions developed for the air environment to implement biometric exit at sea ports. Additionally, the use of mobile technology may be applicable for sea. Sea also encompasses cargo vessels, pleasure boats and boats for hire, which like general aviation present an extremely dynamic environment that will need innovative solutions.

1.3.4 Summary

In the near term, CBP will use Biometric Exit Fee funds to research and develop solutions for air, sea, and land travel environments and deploy exit capabilities in the air environment. Solutions developed for air will be leveraged and adapted for land and sea. CBP will support the establishment of an interconnected and fully functioning enterprise system, upgrade its technical infrastructure, and dedicate program management and related resources to support operations.

1.4 Mission Support Capability Description

Figure 2 depicts the relationship of the operational areas/organizations to the required capability - Verify Traveler Identity, Create/Manage Biometric Records and Report.

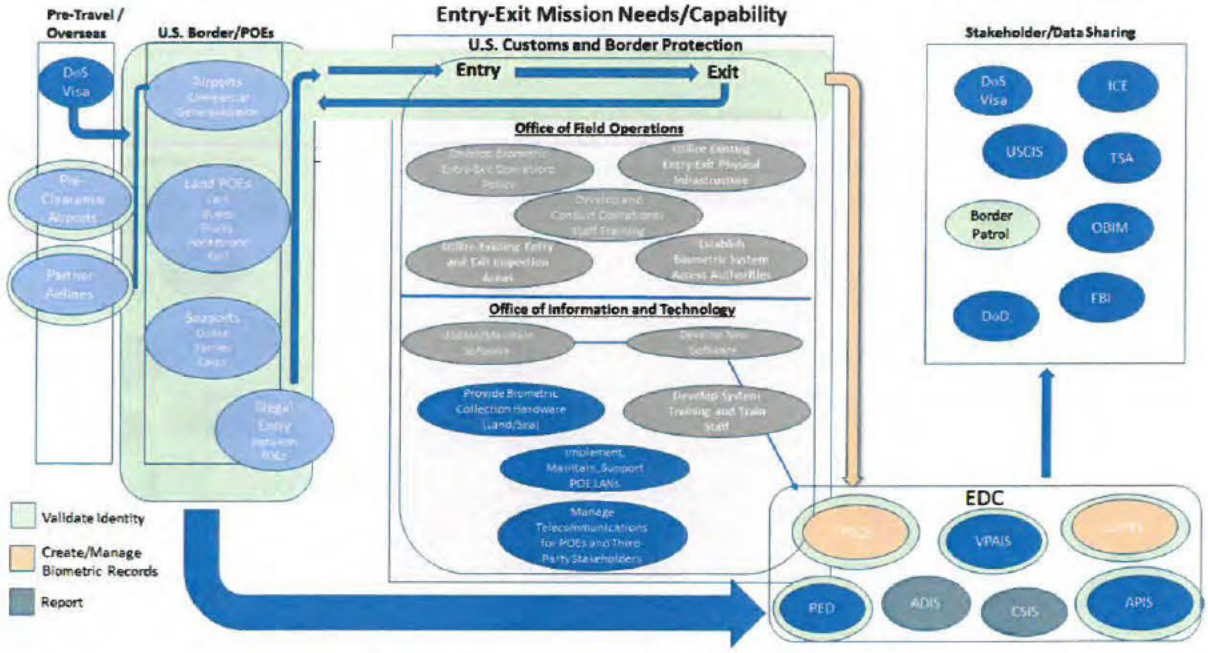


Figure 2 - Organizations Supporting Capability Requirements

The mission support function is distributed across the DHS and CBP communities, using enterprise systems and support communities to ensure effective program support. Biometric Entry-Exit will monitor and oversee the critical support activities of its Mission Support partners using appropriate standards, quality metrics and measurements to ensure compliance. The following sections discuss the Mission Support partners and their respective roles.

1.5 Mission Support Partners

Figure 3 highlights the mission support areas required to meet the needed capabilities. Since Biometric Entry-Exit is primarily a non-materiel system and uses DHS Enterprise Services, many of the mission support functions are defined within the organizational mission areas for a specific service function. For example, DHS OneNet and Network Operations Center (NOC) provide the telecommunications backbone and operational support for not only Biometric Entry-Exit, but all of CBP and each has its own mission support plan and organization. Biometric Entry-Exit uses the Service Level Agreements and logistics support metrics defined and supported by OneNet and NOC to monitor system performance to ensure compliance[10]. Biometric Entry-Exit also uses the Enterprise Data Centers (EDC) to support its computing and data storage needs. EDC follows its enterprise level support functions defined by metrics for

[10] The DHSConnect IT Services and Hardware web page details the service offerings and objectives for customer support for enterprise services provided by DHS.

availability, reliability and performance, which are detailed in the Biometric Entry-Exit Program Operational Requirements Document (ORD).

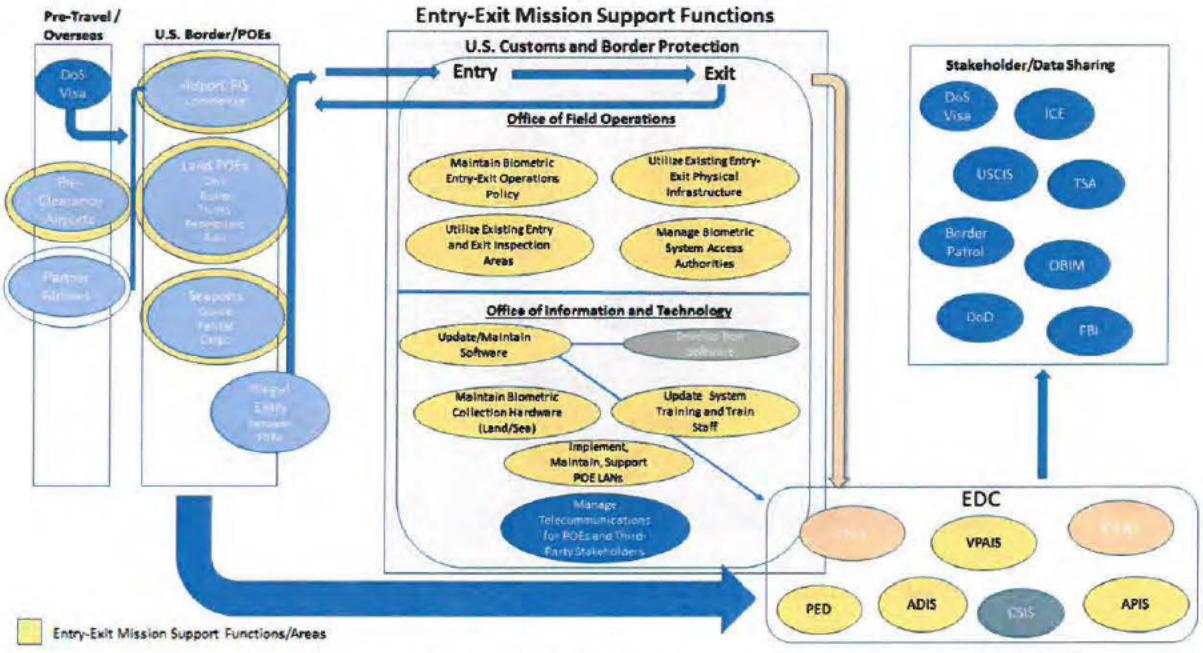


Figure 3 – Mission Support Functional Areas

The detailed mission support functions are defined and carried out by the appropriate organization within the Mission Support Community.

1.6 Mission Support Community

The Mission Support Community includes a range of organizations from DHS enterprise organizations to the local technical and facility organizations at the ports of entry. Entry-Exit will define the operational standards, Service Level Agreements (SLA), metrics and reporting requirements to monitor operations and ensure compliance. Biometric Entry-Exit will use DHS enterprise provided services for wireless and telecommunications, data center operations and data storage and warehousing and their associated support structures. CBP OIT will provide application development and maintenance services for the biometric system operations while the OFO Office of Facilities will support the required changes in the Airport Federal Inspection Service (FIS) areas, land border POEs and seaports to meet the program requirements. Training will be developed and delivered by CBP OFO and OIT. CBP Officers will be trained on system functionality and the operational procedures which govern the use of biometric capture and responses to biometric matching results.

Table 9 identifies the support category, the responsible organization and users, and the program's role.

Table 9 – Categories, Organizations, Users and Entry-Exit Mission Support Role

Category	Responsibility	User Group(s)	Entry-Exit Role
DHS Enterprise Level			
Logistics Management	OneNet/NOC EDC	Telecom/Wireless Managers, Planners Hardware and Data System Designers and Managers	Set Performance Standards, Metrics, SLAs Monitor through performance compliance reporting
Logistics Engineering	OneNet/NOC EDC	Telecom/Wireless Engineers and Technicians, Analysts Hardware Engineers, Data Collection and Storage Analysts and Engineers, Data Technicians	Set Performance Standards, Metrics, SLAs
Support and Test Equipment	OneNet/NOC EDC	Telecom/Wireless Support Managers, Engineers, Analysts Hardware Support and Test Engineers, Data Collection and Storage Analyst and Engineers, Data Technicians	Set Performance Standards, Metrics, SLAs
Supply and Distribution Management	OneNet/NOC EDC	Telecom/Wireless Supply Managers and Engineers Computer Hardware Managers and Engineers	Set Performance Standards, Metrics, SLAs
Technical Data	EDC	Data Managers, Analyst Technicians	Set Performance Standards, Metrics, SLAs
CBP Level			
Information Technology	OIT	System Analysts, System Engineers, Software Developers, Software Maintainers, Data Base Designers and Developers, Security Analysts, Documentation Specialists	Define/Manage Requirements Monitor requirements compliance through weekly meetings, reports to ensure

Category	Responsibility	User Group(s)	Entry-Exit Role
Logistics Management	OIT	System Planners, Hardware Acquisition Managers	Define/Manage Requirements Monitor requirements compliance
Support and Test Equipment	OIT	Hardware Engineers, Test Engineers	Define Requirements Monitor requirements compliance through reporting
Supply and Distribution Management	OIT (Biometric Data Collection Devices)	Supply Management Specialists	Define Requirements Monitor requirements compliance through reporting
Infrastructure	OFO Facilities Management (Ports of Entry, Federal Inspection Areas)	Facility Designers, Construction Managers, Facility Maintainers	Define Requirements Monitor requirements compliance through reporting
Manpower and Personnel	OIT	Hardware Engineers, Software Developers, Contract Support	Develop Operational Staff Estimates and Requirements
Training and Trainers	OIT	System Training Managers, Curriculum Developers, Trainers	Operational Training Developers, Trainers
Combined			
Maintenance	OneNet, EDC, OIT	Maintenance Planners, Analysts (Hardware and Software) Documentation Specialists	Define Requirements Monitor requirements compliance through reporting

1.6.1 Technical

A common backend infrastructure will support processing in all travel modalities (air, land, and sea) requiring acquisition of ongoing operations and maintenance contracts to support expanded networks, systems and applications.

1.6.2 Staffing

Sufficient staffing will be required to ensure that the collection, analysis and enforcement of the newly implemented capabilities are properly supported. This will require additional hiring plus retraining of current staff. Utilization of public/private partnerships will minimize CBP staffing needs to support front-end biometric capture devices.

1.7 Current Situation

There is a significant gap between the end-state vision and current capabilities. Table 10 summarizes the capabilities gaps for Air, Land and Sea operational environments with respect to processing exiting travelers. This assessment is based on an analysis of current CBP operations and capabilities to process travelers as they exit the country by air, land, and sea.

Table 10 – Summary of Outbound (Exit) Capabilities Gaps

Exit Environment	Infrastructure Gaps	Technology Gaps	Operational & Policy Gaps
Air & Sea	• No central point of departure control • No infrastructure for departure control (Space, IT, Network) • Facilities infrastructure varies from port to port • No signage for CBP exit processes	• No unmanned capability in place to biometrically verify exiting travelers • Current biometric capabilities on outbound do not offer the facilitation benefit required to minimize impact to exit processes (no impact to boarding times) • No automated capability to alert officers of enforcement events when departing	• Current processes and policies do not fully support exit processing utilizing biometrics • Tailored Outbound Enforcement Policies do not exist • No operational support for outbound traveler adjudication
Land	• No infrastructure for departure control (Space, IT, Network) • Facilities infrastructure varies from port to port • No signage for CBP processes	• No unmanned capability in place to biometrically verify exiting travelers • Current biometric capabilities on inbound do not offer the facilitation benefit required to minimize impact to exit processes (no backup departing the land border) • No automated capability to alert officers of enforcement events when departing	• Current processes and policies do not fully support exit processing utilizing biometrics • Tailored Outbound Enforcement Policies do not exist • No operational support for outbound traveler adjudication

2 Operations and Support Description

2.1 Missions (Primary/Secondary)

Table 11 identifies the primary and secondary contributions of the Biometric Entry-Exit Program to CBP missions and identifies the key users involved in each mission.

Table 11 – CBP Mission Contributions

CBP Mission	Primary/ Secondary	Users
Counter Terrorism and Transnational Crime • Enhance Procedures and Partnerships • Increase Situational Awareness of Air, Land and Sea	Primary	CBP Officers
Advance Comprehensive Border Security and Management • Detect, Interdict, and Disrupt Illegal Cross-Border Activities • Conduct Outbound Enforcement and Interdiction of Travelers	Primary	CBP Officers
Enabling Lawful Trade and Travel • Identify Travel Threats as Early as Possible • Reduce Costs for U.S. and Trade and Travel Communities • Expand Risk-Segmentation to Enable Low-Risk Travel	Primary	CBP Officers, Travel Industry Stakeholders, Traveling public
Promote Organization Integration, Innovation, and Agility • Advance CBP Mission Effectiveness	Secondary	CBP, Travel Industry Stakeholders

2.2 Users and Other Stakeholders

2.2.1 Users

Users of the biometric entry-exit program include the traveling public and U.S. Customs and Border Protection Officers.

- Traveling Public—will allow biometric images to be captured by stakeholders' front-end biometric capture devices during entry and exit and then securely submitted to CBP for matching.

- U.S. Customs and Border Protection Officers—will respond to law enforcement hits generated by the biometric entry-exit system to make informed decisions about travelers entering or exiting the country.

2.2.2 Government Stakeholders

Government stakeholders of the Biometric Entry-Exit program include the primary organizations who operate and support the program, organizations that are sources of biometric data for matching, and organizations that can leverage biometric entry-exit crossing records for their own mission needs. CBP will leverage existing biometric data holdings in government systems to build galleries for matching. Additionally, CBP will provide biometrically confirmed crossing records of in-scope, non-U.S. citizen travelers to OBIM that can be leveraged by other government agencies to fulfill their mission needs.

Primary Stakeholders:

- DHS/CBP (Office of Field Operations) – will manage the operations of the program.
- CBP Office of Information and Technology (OIT) – will develop, deploy and provide mission support for the technical solution.
- DHS Enterprise Services – Leverage common biometric capabilities.

Biometric Data Source Stakeholders:

- DHS OBIM – DHS primary biometric data repository; primary source of biometric data; will record biometrically confirmed crossings of in-scope, non-U.S. citizen travelers.
- State and Federal Agencies including Department of State (DoS) and USCG – will share biometric data.
- USCIS – will share biometric data.
- CBP – Other photos sources may include APC, CEAC, CIS, GES, VISA, and EID.

Stakeholders who can leverage Biometric Entry-Exit Program data:

- TSA – can utilize TVS to identify travelers entering their security checkpoints eliminating the need to check IDs and boarding passes.
- ICE – will leverage biometric entry-exit crossing records for their mission needs that includes criminal and administrative enforcement.
- DHS/CBP (Border Patrol) – can leverage biometric entry-exit crossing records for their mission needs.
- U.S. Coast Guard – can leverage biometric entry-exit crossing records for their mission needs.

2.2.3 Non-Government Stakeholders

Non-Government stakeholders from the travel industry will provide passenger manifest data to CBP in advance of travel allowing CBP to create logical or physical galleries to perform real time matching at border crossing. Additionally, travel industry partners in air and sea will integrated front-end biometric capture devices into their boarding processes to provide live biometric images to TVS for adjudication and processing. Non-Government stakeholders include:

- Commercial Airlines - will continue to provide APIS manifest data as well as securely submit live biometric images collected from travelers to CBP systems for adjudication and processing.
- Airport Authorities - may securely submit live biometric images collected from travelers on behalf of airlines to CBP systems for adjudication and processing.
- Commercial Cruise Lines - will continue to provide APIS manifest data as well as securely submit live biometric images collected from travelers to CBP systems for adjudication and processing.
- Commercial Bus Lines – will provide passenger manifest data to CBP in advance of travel.

2.3 Policies, Assumptions and Constraints

2.3.1 Policy

Current privacy policies and regulations allow for the collection and recording of biographic data and the collection and matching of biometrics on in-scope non-U.S. citizens travelers for both entry and exit (8 USC § 1365b (d) (f)). Legal authorities for CBP to collect and utilize biographic and biometric data to confirm identity at the time of arrival to and departure from the United States include:

- Immigration and Nationality Act (INA) § 235 [8 USC 1225], § 287 [8 USC 1357] and § 215 [8 USC 1185]
- 8 CFR § 215.8 Requirements for biometric identifiers from aliens on departure from the United States
- 8 CFR § 235.1 Scope of examination
- 8 CFR § 235.1(b) Requirement for U.S. citizen to possess valid U.S. passport for entry to or departure from the U.S. (see also 8 CFR 1185(b))
- 8 CFR § 235.1(f) Alien applicants for admission
- 8 USC § 1187(i) Visa Waiver Program; Establishment of exit system
- 8 USC § 1365b(d)-(h) Biometric entry and exit data system; Collection of biometric exit data; Integration and interoperability; Maintaining accuracy and integrity of entry and exit data system; Integrated biometric entry-exit screening system; Entry-exit system goals

- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 7208 and 7209, as amended (P.L. 108-458)
- The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, P.L. 107-56, Sec 414(b))
- Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6)
- Department of Homeland Security Appropriations Act, 2015 (P.L. 114-4)
- Consolidated Appropriations Act, 2016 (P.L. 114-113)
- January 2004 Interim Final Rule (69 FR 468) on Non-Immigrant Visa Travelers
- Exit pilots were established in this rule, and updated later in 2004 in 69 FR 46556 and 69 FR 51695.
- August 2004 Interim Final Rule (69 FR 53318) on VWP Travelers and 50 Largest Land Ports
- 50 Largest Land POEs identified in November 2004 (69 FR 64964)
- Remaining Land POEs identified in September 2005 (70 FR 54398)
- December 2008 Final Rule (73 FR 77473) on Additional Alien Categories
- June 2009 Notice (74 FR 26721) on Biometric Air Exit Pilot at Two Airports
- July 2015 Notice (80 FR 44983) BE-Mobile at top 10 airports
- November 2015 Notice (80 FR 70241) Otay Mesa Field Trial
- Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States" Sec. 8. Expedited Completion of the Biometric Entry-Exit Tracking System (March 6, 2017)
- Storage of traveler's biometric and biographic data and duration of holding is covered by:
- DHS/CBP-007 Border Crossing Information (BCI) System of Record Notice (SORN) of July 25, 2008;
- DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) SORN June 5, 2007;
- DHS/CBP-011 U.S. Customs and Border Protection Travelers Enforcement Communications System (TECS) SORN of December 19, 2008.

2.3.2 Assumptions

- Deployment of exit capability to airports will require public/private partnerships. Private parties who agree to participate will be prioritized for deployment.
- Airlines and airports will own and maintain the devices to capture and securely submit biometrics to the TVS per CBP specifications.
- All backend system and infrastructure capabilities must be fully functional and scalable prior to deployment for the first flights.

- The biometric exit solution will interface with DHS OBIM to provide biometrically confirmed exit records for in-scope, non-U.S. citizen travelers. In the long term, DHS OBIM will provide biometrically verified Entry and Exit transactions to the CBP ADIS as an alternative to TVS directly updating ADIS.
- Outbound policies and procedures will be updated and approved in compliance with all DHS policies.

2.3.3 Constraints

- The Biometric Exit Fee Fund will apply to IT investment, programmatic and operational support, additional CBP Officer staffing for outbound enforcement, and technology innovation to provide biometric exit capabilities.
- Many ports do not have a brick and mortar facility for vehicle or pedestrians exiting the U.S. Port configuration may be a limiting factor as to the type and extent of the solution that will be viable.
- Provide appropriate accommodation for individuals wearing religious headwear (e.g., individuals whose headwear may need to be adjusted to take the photograph), in line with Department policy on accommodation of religious beliefs in fingerprinting and photography.
- Provide appropriate accommodation of individuals who do not take photographs for religious reasons (see, related, the 2009 guidance on accommodation of the Amish in implementation of WHTI).
- Provide accommodation of individuals without fingers/fingerprints due to injury/disability.
- CBP will ensure privacy and compliance with all applicable laws according to DHS policy.

2.4 Operational Description

CBP's transformative Biometric Pathway vision will utilize biometrics as an alternative to biographics as the key to unlocking a known traveler's record throughout the travel process. A common approach from a user-oriented perspective will be established for air, land, and sea environments supporting border crossings. To achieve the Biometric Pathway Vision, CBP will implement a biometric matching capability called the Traveler Verification Service (TVS) to be used by travel industry stakeholders or by CBP itself to identify travelers throughout the travel process. Figure 4, Level 1 Operational View, illustrates how TVS, a biometric matching service, will support all modes of travel for exit. Regardless of mode of travel, front-end biometric capture devices will capture live biometrics to securely submit to TVS for processing and adjudication.

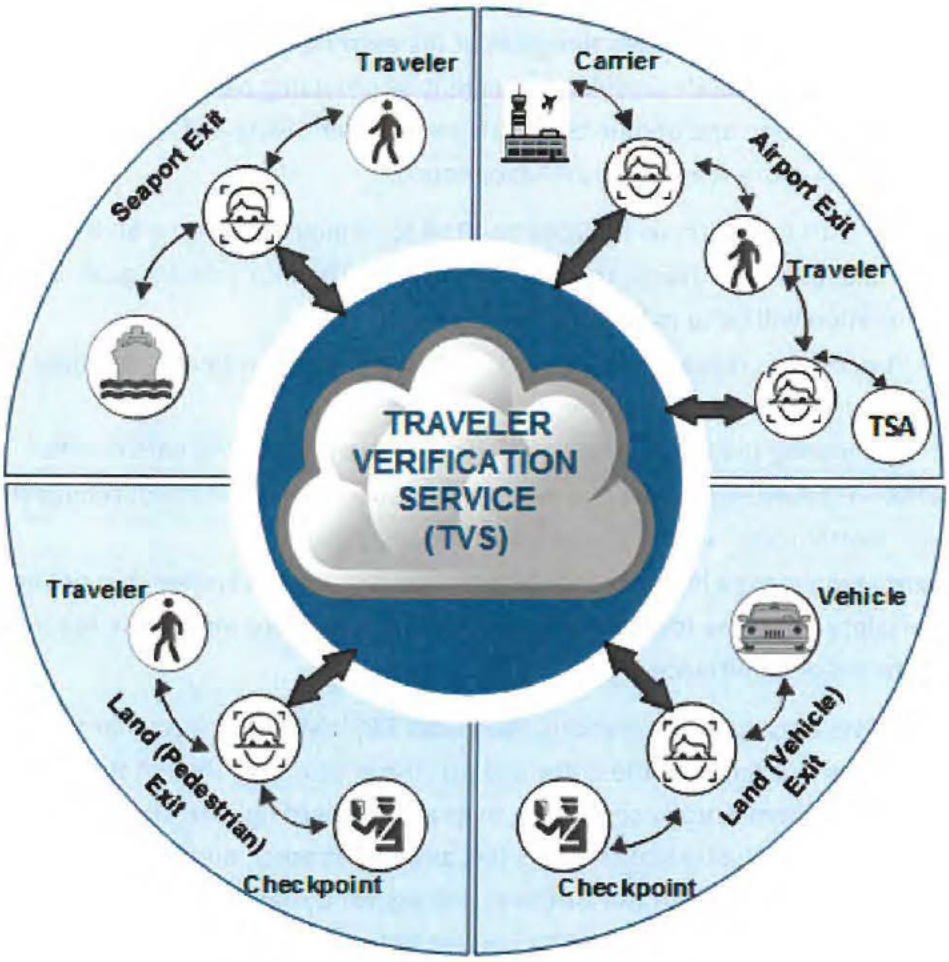


Figure 4 - Level 1 Operational View

The following sub-sections identify the proposed solution from a user-oriented perspective in operational settings for air, land and sea environments. Air is the first priority for implementing biometric exit. Biometric exit solutions for land and sea will follow, leveraging solutions and lessons learned from deployment of an air exit program.

2.4.1 Air

The concept of operations for air travel aligns with CBP's Biometric Pathway vision. The Biometric Pathway vision will transform the way CBP identifies air travelers by shifting the key to unlocking a traveler's record from biographic identifiers to biometric ones – primarily a traveler's face. Pre-staging the existing traveler data upstream in the travel process enables all stakeholders to transform from manual and redundant processes to safer, automated, and seamless traveler movement. CBP can continue to increase security by using a live facial biometric to match the traveler to advance passenger information, while also checking any

existing fingerprints on file against the watch list, which decreases dependency on less reliable paper travel documents, such as Passports and Visas. New facial recognition processes will enhance CBP's biometric capabilities alongside of the existing 10-print fingerprint processes. This approach will also facilitate traveler movement by providing partners – airlines, airports, and TSA – with a common and unique biometric key for identifying and matching travelers to identities, creating a more seamless travel experience.

CBP will partner with the air travel industry and TSA to deploy a biometric air entry/exit solution that transforms the overall traveler experience. The four primary goals of this large-scale transformation will be to make air travel more:

- **Secure** - Providing increased certainty as to the identity of travelers at multiple points in the travel continuum;
- **Simple** - Eliminating the need for physical document and boarding pass checks;
- **Facilitative** - Establishing a clear and easily understood process that will reduce the potential for major "bottlenecks" within the air travel process; and
- **Compliant** - Employing a high integrity biometric entry and exit system that not only increases CBP's certainty as to the identity of travelers, but also more ably holds accountable those violating terms of admittance.

Figure 5, Air Travel Concept of Operations, illustrates CBP's vision of future air travel utilizing biometric identifiers throughout the entry and exit travel process. Though the core biometric exit capability is for biometrically confirming exits at the boarding gate, there is a potential opportunity for travel industry stakeholders (i.e. airlines, airports, and TSA) to utilize this capability at all steps throughout the air travel process for a seamless and token-less traveler experience where travelers do not need to present boarding passes or travel documents. The initial capability is for implementation of biometric capabilities at the boarding gate to biometrically confirm exits. In the future, air travel partners may elect to integrate biometric capabilities at other steps in the travel process. Implementation by CBP of biometric verification at bag drop is a future capability consideration.

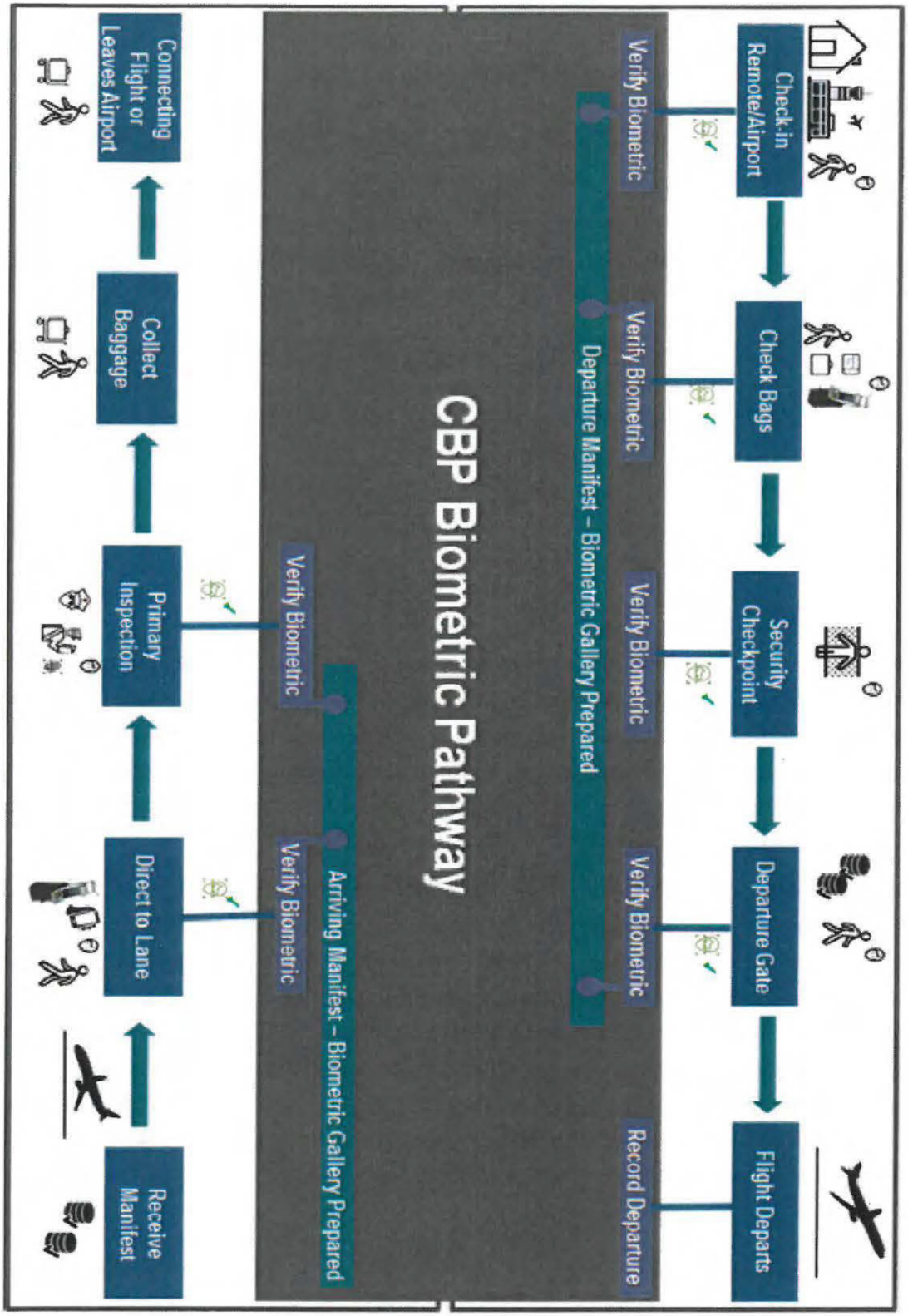


Figure 5 - Air Travel Concept of Operations

To successfully implement the Biometric Pathway, CBP will accomplish the following:

1) Reengineer and re-design CBP data handling;
2) Build a communication portal to connect with partners;
3) Implement a Traveler Verification Service (TVS) for one-to-many biometric searching; and
4) Implement a mechanism to provide wayfinding and lane assignments prior to entry.

CBP will ensure privacy and compliance with all applicable privacy policies, procedures and internal controls necessary to safeguard PII pursuant to the Privacy Act.

2.4.1.1 Air Operating Concept

The following sub-sections describe the air operating concept for both departure and arrival that are in alignment with CBP's Biometric Pathway vision. Implementing CBP's Biometric Pathway vision for transforming the traveler's overall experience will require collaboration from CBP, TSA, and both the airline and airport industry. CBP will provide TVS, a backend biometric matching service, to enable stakeholders to optionally automate their manual processes by deploying front-end solutions to capture and securely submit live biometrics of travelers to CBP.

2.4.1.1.1 Air Departure

Airlines, Airports and TSA can optionally integrate TVS throughout the travel process (such as at check-in, bag drop, and TSA checkpoint) to biometrically identify travelers creating a seamless and token-less experience for the traveler without the need to present a boarding pass or travel document. While biometric matching will be optional throughout the travel process prior to boarding, CBP will require capture and submittal of live biometric images at aircraft boarding so that CBP can meet its mission of biometrically confirming exits.

Biometric exit will also include an updated outbound enforcement policy specifically focused on those violations that warrant an enforcement action for an individual departing the United States. If any threats are identified at the time of boarding a flight departing the United States, the biometric exit system will alert CBP outbound enforcement teams by sending a message to a mobile device. Teams will respond to adjudicate the issue. Outbound policy will address how to resolve non-law enforcement related exceptions such as failure to capture a live biometric image and failure to match to biometric images of expected travelers on the flight manifest. The system will also have the capability to provide calling entities with the traveler's biometrically confirmed identity and authorization to proceed.

2.4.1.1.2 Air Arrival

As stated with the departure, the air arrival end state vision will require collaboration from CBP, TSA, and both the airline and airport industry. Essentially, the arrival concept uses similar services to streamline or eliminate processes that currently impact arrival processing. If

biometrics are optionally captured at the international check-in, they can be utilized upon arrival for an improved passenger experience.

2.4.1.2 Air Employment Modes

TVS must reliably provide real time responses to calling entities (airlines, airports, TSA, or CBP itself) within times that will not impede the air travel process for how it is utilized at check-in, bag drop, TSA, and boarding. The solution must be capable of scaling to perform biometric matching services for all international departing flights. The solution will be scaled to match stakeholders' deployments of front-end biometric capture devices. The solution must also be capable of scaling to perform biometric matching services for all international arrivals as stakeholders deploy front end solutions supporting entry.

2.4.1.3 Air Scheduling and Operations Planning

To prevent disruptive impacts to trade or travel, TVS capabilities will require mission critical high availability and system redundancies to support 24/7 operations and minimal planned maintenance outages. In the event of a system outage preventing TVS from functioning at full capacity, a contingency plan will be developed to provide stakeholders direction for processing travelers.

2.4.1.4 Air Operating Environment

2.4.1.4.1 Geographic Areas

CBP will deploy TVS, a back-end biometric matching service, capable of supporting air travel from any airport with international flights to and from the United States and its territories. Stakeholders (Airlines, Airports, TSA and possibly CBP itself) are responsible for connecting their front-end biometric capture devices to TVTVS.

2.4.1.4.2 Environmental Conditions

CBP will deploy TVS, a back-end biometric matching service, to support front-end biometric capture devices deployed by stakeholders. The front-end solutions are expected to operate inside Airport buildings. Stakeholders are responsible for adapting their front-end systems to environmental conditions at specific airports.

2.4.1.4.3 Operational Conditions

The CBP TVS will operate in a secure and controlled data center environment rated for high confidentiality, high integrity and high availability minimizing physical risks and hazards to the service.

Upon arriving at a location where a biometric facial image will be captured, the traveler confronts one of three configurations:

- An operator ready to provide active assistance to the traveler for capturing a photo

- A direct interface with the camera device with passive assistance from an operator
- A direct interface with a camera without any operator assistance

In all cases, signage and instructions are to be provided to the traveler. Performance requirements, workload drivers, and safety hazards for the operator and traveler are to be addressed by the entity operating the camera.

A CBP officer may be required to respond to a traveler for law enforcement activities. In this instance, CBP officers receive notifications on an existing mobile device and will respond according to existing policies and procedures.

2.4.2 Land

The CBP land border entry and exit concept of operations will leverage solutions developed for other environments such as air and sea as well as new technology necessary due to the complex landscape along the land border. Travelers entering the United States via the land border arrive primarily in Privately Owned Vehicles (POV), commercial buses and on foot. Ferry and rail travelers are also classified as land travelers. Feasible operational concepts for land are currently being developed and experiments are ongoing. This CONOPS will be updated as solutions for land are further identified.

2.4.2.1 Land Operating Concept

Notionally, the operating concept for each environment will be:

POV Entry - As a POV proceeds down the primary lane, a License Plate Reader (LPR) will photograph the vehicle license plates and a camera will capture an image of the driver (and possibly the passenger as well) through the vehicle windshield. CBP will attempt to match the image taken in the primary lane with images in DHS holdings to verify the identity of the driver. Once the identity of the driver and all passengers are verified, the CBP Officer will make an admissibility determination and the traveler(s) will be either admitted into the United States or referred for secondary inspection.

POV Exit – As stated above, the infrastructure at land POEs does not support exit processing. Additionally, the majority of travelers exiting the United States by POV are not subject to the collection of biometrics. CBP therefore will place the burden of reporting on the traveler using a mobile or kiosk-type solution[11]. A traveler would physically report to a kiosk or use features such as location services on a mobile device to satisfy CBP that they have indeed left the country. Additionally, data exchanges with Mexico and Canada would serve to validate the departure of in-scope travelers.

[11] Various solutions are being evaluated in test environments, but no single solution or set of solutions have been selected for operational deployment.

Pedestrian Entry – A camera would capture an image of a pedestrian's face and attempt to compare that image against a pre-established database (conceptually similar to a manifest). Once the identity of the traveler has been verified, the CBP Officer would make an admissibility decision.

Pedestrian Exit – As noted in POV exit, CBP would establish the capability for a traveler to self-report. Travelers that fail to self-report would be considered overstays and, consequently, ineligible for re-entry.

Bus Entry – An image of a bus passenger would be captured and compared to a manifest. Once the identity of the traveler is verified, a CBP Officer would make an admissibility determination.

Bus Exit – A bus exit concept, while not fully developed, has features of air (there is a manifest), and land (there could be a self-reporting capability).

2.4.2.2 Land Employment Modes

Biometric entry-exit solutions at land ports must not impede the travel process. The solution should be capable of scaling to support traffic at all land Ports on the Mexican and Canadian borders.

2.4.2.3 Land Scheduling and Operations Planning

To prevent disruptive impacts to port operations or to trade and travel, biometric exit solutions for land ports will require mission critical availability with 24/7 operations and minimal planned maintenance outages. In the event of a system outage preventing biometric confirmations, a contingency plan is needed to provide Ports direction for processing travelers.

2.4.2.4 Land Operating Environment

2.4.2.4.1 Geographic Areas

Biometric Exit solutions for land must function at POEs on both the Northern and Southern borders.

2.4.2.4.2 Environmental Conditions

Environmental conditions at land POE's range from subzero temperatures to significant snowfall to one hundred degree plus temperatures and sunlight and glare. Inspection processing occurs indoors as well as outdoors at all times of the day and night, so any deployed capability must have the ability to operate in all outdoor conditions.

2.4.2.4.3 Operational Conditions

Any deployed capability must be ruggedized due to the environmental conditions and due to the fact they will be engaged by the traveling public. Technology in vehicle lanes is subject to being hit by vehicles.

2.4.3 Sea

The concept of operations for sea travelers exiting the country will follow the same concept as air travelers and leverage solutions developed for the air environment. Public/Private partnerships with sea carriers will be explored for implementation of front-end biometric capture solutions.

2.4.3.1 Sea Operating Concept

Sea travelers will present biometrics to the cruise line upon embarkation.

The following steps identify the end state operational process for commercial sea travelers:

Embark at Sea Port

1. CBP utilizes APIS manifest data to develop small searchable photo galleries of sea travelers.
2. The cruise line or CBP captures biometrics on all travelers prior to embarkation
3. Match live biometrics to existing traveler biometrics
   a. For a successful match, record exit for in-scope, non-U.S. citizen travelers as biometrically confirmed
   b. For an unsuccessful match, perform biographic match and record exit as biographically confirmed
   c. Alert traveler when process is complete
4. If a match is made to an identity with actionable biometric or biographic watch list hits, or the traveler is determined to be a person who originally entered the U.S. without inspection, provide mobile alerts to CBP Officers to respond in accordance with exit policy

2.4.3.2 Sea Employment Modes

Biometric exit solutions at sea ports must not impede the travel process. The solution should be capable of scaling to support exit traffic at all sea ports.

2.4.3.3 Sea Scheduling and Operations Planning

To prevent disruptive impacts to trade or travel, biometric exit solutions for land ports will require mission critical availability with 24/7 operations and minimal planned maintenance outages. In the event of a system outage preventing biometric confirmations, a contingency plan will be developed to provide Ports direction for processing travelers.

2.4.3.4 Sea Operating Environment

2.4.3.4.1 Geographic Areas

Biometric Exit solutions must function at all sea ports.

2.4.3.4.2 Environmental Conditions

Environmental conditions at Sea POE's range from subzero temperatures to significant snowfall to one hundred degree plus temperatures and sunlight and glare. Inspection processing occurs indoors as well as outdoors at all times of the day and night, so any deployed capability must have the ability to operate in all outdoor conditions.

2.4.3.4.3 Operational Conditions

Biometric Exit solutions for sea will operate in a variety of conditions. Each port where biometric exit solutions are deployed will need to be assessed for physical risks and hazards requiring mitigation.

2.4.4 Threats and Hazards

The CBP TVS will be available for use by authenticated and authorized stakeholders' front-end biometric capture devices. The greatest threats to the system are cybersecurity threats from unauthorized actors with the greatest risk being data breaches of sensitive PII maintained by the system. Security and privacy controls following NIST 800-53 guidance for high impact systems are to be implemented to provide safeguards and countermeasures designed to protect the confidentiality, integrity, and availability of the biometric entry-exit system and its information.

2.4.5 Interoperability with Other Elements

TVS capability for entry-exit will build upon existing DHS, CBP and other government systems. Biometric Entry-Exit will interface with existing systems to build biometric galleries using existing government holdings, biographically and biometrically search watch lists, biometrically confirm crossings, and match arrival and departure records. Figure 6, system interoperability, identifies key interfaces to other systems and the types of data interchanged.

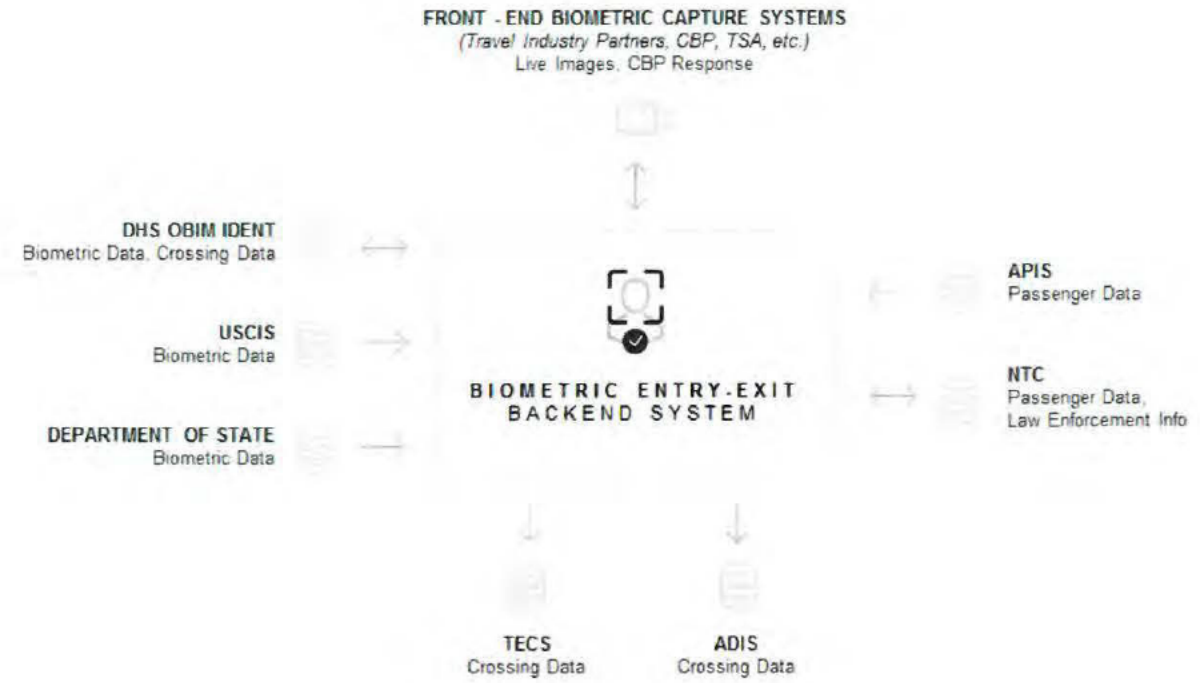


Figure 6 – System Interoperability

Airlines, cruise lines, bus lines, and rail will utilize APIS to provide biographic passenger manifest data prior to travel. The APIS manifest data will be used to create matching galleries and pre-adjudicate travelers. DHS OBIM IDENT/HART, USCIS, and Department of State are key sources for biometric information used to build searchable galleries. The National Targeting Center (NTC) will utilize biometric exit data for threat assessments. DHS OBIM IDENT/HART, TECS and ADIS will biometrically record border crossings for all in-scope, non-U.S. citizen travelers.

2.5 Mission Support Description

This section addresses the mission support functions, concept and organization necessary for both immediate and continued operation of the Biometric Entry-Exit Program to meet mission needs.

2.5.1 Key Support Areas

The key mission support areas within Entry-Exit consist of governance and management requirements addressing policy, strategic planning, innovation, financial management, communications and stakeholder management, oversight of acquisitions, engineering and logistics, and communications management. Each of these functions contributes to system readiness and the efficiency and effectiveness of mission support delivery in the field.

- ***Policy development*** will ensure that Entry-Exit is meeting its legal, regulatory, fiduciary responsibilities, and religious and disability accommodations. It involves developing policy

and procedures to set and control standards, guide internal program administration and procedures, train personnel, and translate lessons learned into organizational change.

- ***Strategy setting*** will equip Entry-Exit to overcome future challenges and take advantage of new opportunities. It involves making strategic decisions about the future of the Program's mission support role and developing and promulgating performance goals and standards that, when coupled with operational requirements, inform the prioritization of mission support resources for future capabilities.
- ***Planning, programming, and budgeting*** will provide Entry-Exit with the resources required to support CBP border security and immigration missions and advance the strategic goals of the organization. These functions involve acquiring resources through the Federal budget process and developing plans and budgets for the allocation of those resources.
- ***Participation in, and oversight of, major acquisitions***, based on the program's relationships and proximity to partners, stakeholders, and other resources will ensure that the resources being acquired meet program requirements.
- ***Communications and stakeholder management*** will consist of outreach to other governmental entities, both foreign and domestic, as well as management of both international and domestic airline carriers and cruise lines on biometric exit.
- ***Guidance, support and oversight*** will oversee the technical and logistics aspects of Entry-Exit operations, maintenance and sustainment and provide the standards and performance requirements for all systems and assets, which are carried out by the operational teams supplied through separate organizations within CBP.

Table 12 depicts the major categories of support, responsibilities of the mission support organizations and associated user groups, and the program's role to address the key support areas identified above.

Table 12 – Mission Support Functions and Roles

Category	Responsibility	User Group(s)	Entry-Exit Role
DHS Enterprise Level			
Logistics Management	OneNet/NOC EDC	Telecom/Wireless Managers, Planners Hardware and Data System Designers and Managers	Set Performance Standards, Metrics, SLAs Monitor through performance compliance reporting
Logistics Engineering	OneNet/NOC EDC	Telecom/Wireless Engineers and Technicians, Analysts Hardware Engineers, Data Collection and Storage	Set Performance Standards, Metrics, SLAs

Category	Responsibility	User Group(s)	Entry-Exit Role
		Analysts and Engineers, Data Technicians	
Support and Test Equipment	OneNet/NOC EDC	Telecom/Wireless Support Managers, Engineers, Analysts Hardware Support and Test Engineers, Data Collection and Storage Analysts and Engineers, Data Technicians	Set Performance Standards, Metrics, SLAs
Supply and Distribution Management	OneNet/NOC EDC	Telecom/Wireless Supply Managers and Engineers Computer Hardware Managers and Engineers	Set Performance Standards, Metrics, SLAs
Technical Data	EDC	Data Managers, Analyst Technicians	Set Performance Standards, Metrics, SLAs
CBP Level			
Program Management	OFO	Program Managers, Policy SMEs, Requirements SMEs, Financial SMEs	Define Requirements Maintain Biometric Entry-Exit Policy Manage Biometric System Access Authorities Maintain Budget Stakeholder engagement
Information Technology	OIT	System Analysts, System Engineers, Software Developers, Software Maintainers, Data Base Designers and Developers, Security Analysts, Documentation Specialists	Manage Requirements Monitor requirements compliance through weekly meetings, reports to ensure
Logistics Management	OIT	System Planners, Hardware Acquisition Managers	Define/Manage Requirements Monitor requirements compliance

Category	Responsibility	User Group(s)	Entry-Exit Role
Support and Test Equipment	OIT	Hardware Engineers, Test Engineers	Define Requirements Monitor requirements compliance through reporting
Supply and Distribution Management	OIT (Biometric Data Collection Devices)	Supply Management Specialists	Define Requirements Monitor requirements compliance through reporting
Infrastructure	OFO Facilities Management (Ports of Entry, Federal Inspection Areas)	Facility Designers, Construction Managers, Facility Maintainers	Define Requirements Monitor requirements compliance through reporting
Manpower and Personnel	OIT	Hardware Engineers, Software Developers, Contract Support	Develop Operational Staff Estimates and Requirements
Training and Trainers	OIT	System Training Managers, Curriculum Developers, Trainers	Operational Training Developers, Trainers
Combined			
Maintenance	OneNet, EDC, OIT	Maintenance Planners, Analysts (Hardware and Software) Documentation Specialists	Define Requirements Monitor requirements compliance through reporting

2.5.2 Support Principles

The Mission Support function must adhere to the following principles[12] to ensure success across the operational continuum from the program office, enterprise support organizations to the smallest operational component and support contractor:

- Flexibility - the ability to expand, contract, and adapt to meet changing situations and requirements.
- Responsiveness - the rapid deployment and configuration of resources to fulfill new and evolving requirements, such as those created by a contingency event.
- Resiliency - the ability to withstand changes in the operating environment and expeditiously recover.

[12] The Mission Support principles and MSBM is adapted from the U.S. Coast Guard enterprise MSBM and realigned to meet the specific needs of the Biometric Entry-Exit Program requirements and scope.

- Affordability - the cost-effective achievement of results deemed necessary and appropriate by those supported.
- Transparency - ready access to the data needed to make effective decisions.
- Integration - working cooperatively across all elements of mission support and with diverse governmental and non-governmental entities to support mission requirements.

2.5.3 Mission Support Concept

The Entry-Exit Mission Support concept is driven by a business model approach that will be used by the program office, and promulgated to all supporting technical and logistics organizations, and stakeholders. The Biometric Entry-Exit Program has adopted a MSBM approach from the U.S. Coast Guard that provides a mission-focused, unified, and disciplined approach to mission support delivery. It produces superior service by consolidating accountability, creating a proactive support posture and supporting data-driven decisions. Ultimately, the MSBM contributes to mission effectiveness by optimizing readiness, operational availability, performance, and safety. The MSBM includes product line management, configuration management and asset visibility.

Product Line Management is an organizational design concept that provides a single support team responsible and accountable for the performance of a specific capability's execution and sustainment. Product line management oversees and monitors the configuration of a capability, the activities that sustain that configuration, and prioritizes the allocation of resources based on requirements. This approach breaks down barriers by combining staffs with different functional expertise (e.g., engineering, human performance, resource management, and procurement, etc.) and similar levels of delegated authority (as designated by a community's chain of authority) into a single point of accountability.

Configuration Management (CM) establishes a configuration baseline for a capability that satisfies requirements based on a standard level of service. Throughout a capability's life cycle, as requirements change, changes to the configuration are monitored to ensure a consistent and repeatable process. CM enables a proactive support posture. Knowing the configuration of a system or asset informs what support is needed and how to deliver planned maintenance to sustain it. Proper oversight, standardization, documentation, and monitoring are key characteristics of CM. CM is governed by a cross-functional body that brings together stakeholders with existing program authorities to consider the interdependent impacts of a change. This governance approach will provide community and cultural leadership while ensuring that the support community effectively manages critical changes and acts upon lessons learned.

Asset Visibility collects and analyzes information to create dynamic situational awareness of CBP's Biometric Entry-Exit Program performance in the environments in which it operates.

Information sources include performance measures as well as analysis products (e.g., lessons learned, business case analysis) and the results of compliance checks (e.g., audits, inspections, and assessments). Asset Visibility provides the capability needed to insightfully support, inform, and enable business intelligence and knowledge management.

2.5.4 Mission Support Roles and Responsibilities

Mission Support responsibilities are divided among multiple organizational entities and enterprise business owners. Many components of the program are either provided by outside stakeholders who will follow their own mission support approach (e.g., airlines, TSA) or enterprise level organizations within CBP (OIT, ENTS, Facilities) which also have enterprise mission support plans and organizations that are supported and controlled within the respective organization. The Biometric Entry-Exit Program will provide guidance, operational and performance standards and hold the other entities accountable using the MSBM.

- **Biometric Entry-Exit Program.** The program will implement the MSBM, applying its core elements to govern and manage the end-to-end program key support functions as described in section 2.5.1. Implementing the MSBM will create a culture of continuous learning and improvement that leverages information to control costs, prioritize resources, maintain standards, and improve affordability.
- **External Stakeholders.** In the Air environment, through public/private partnerships, airports, airlines, TSA and potentially other stakeholders will integrate biometric capture devices into their business processes and securely submit biometric images to CBP for matching. This approach prevents CBP from adding additional steps in the travel process requiring a new learned behavior by the traveling public. Stakeholders will benefit from receiving biometrically confirmed identity information of their travelers allowing transformation from biographic identifiers. Mission support of front-end biometric capture devices and connectivity to TVS is provided by stakeholders utilizing the service.
- **CBP OIT.** Mission support for TVS is provided by OIT. This includes all applications and technical infrastructure necessary to successfully operate the service at the required scale and performance parameters.
- **DHS Enterprise Services.** Mission support for leveraged services used in TVS is provided by those leveraged service organizations (i.e. OBIM for leveraged biometric services).

Table 13 provides an overview of the critical functional components of the technical aspects of the system and the organization responsible for primary support.

Table 13 – Mission Support Responsibilities

Biometric Entry-Exit Capabilities		Mission Support Responsibility
Front-End Biometric Capture Devices	Cameras / biometric scanners	Stakeholders (Air/Sea)/ CBP (Land)
	Biometric capture software	Stakeholders (Air/Sea)/ CBP (Land)
	Integration with stakeholders' systems and business processes (if desired)	Stakeholders (Air/Sea)/ CBP (Land)
Port Infrastructure for Front-end Biometric Capture Devices	Network Connectivity to CBP Backend Service	Stakeholders (Air/Sea)/ CBP (Land)
	Signage	Stakeholders (Air/Sea)/ CBP (Land)
	Physical security of front-end biometric capture devices	Stakeholders (Air/Sea)/ CBP (Land)
TVS	Gallery Building	OIT
	Watch list Checks	OIT
	Biometric Matching Service	OIT (or OBIM per the CBP and OBIM Integration Roadmap)
	Automated analysis	OIT
	CBP Officer notifications	OIT
	Biometrically confirmed crossings	OIT
	Dashboards / Reporting / Performance Monitoring	OIT
IT Infrastructure	LAN/WAN	OIT
	Wireless Access for CBP officer notifications	OIT
	Hosting Services	OIT
	DHS Enterprise Services (OneNet, NOC, EDC)	DHS

2.5.5 Mission Support Organization

CBP has established a PMO to manage the Biometric Entry-Exit Program and apply the MSBM. The PMO will develop standards and manage the biometric implementations to ensure biometric exit solutions are integrated with existing travel processes. OIT will provide delivery of TVS along with technical specifications for stakeholders to interface with the biometric matching service. Where DHS Enterprise Services are leveraged, the DHS Enterprise Services delivery organizations will provide mission support for their components.

Figure 7 illustrates how CBP is organized to support the Biometric Entry-Exit mission and identifies the shared program management and mission support functions.

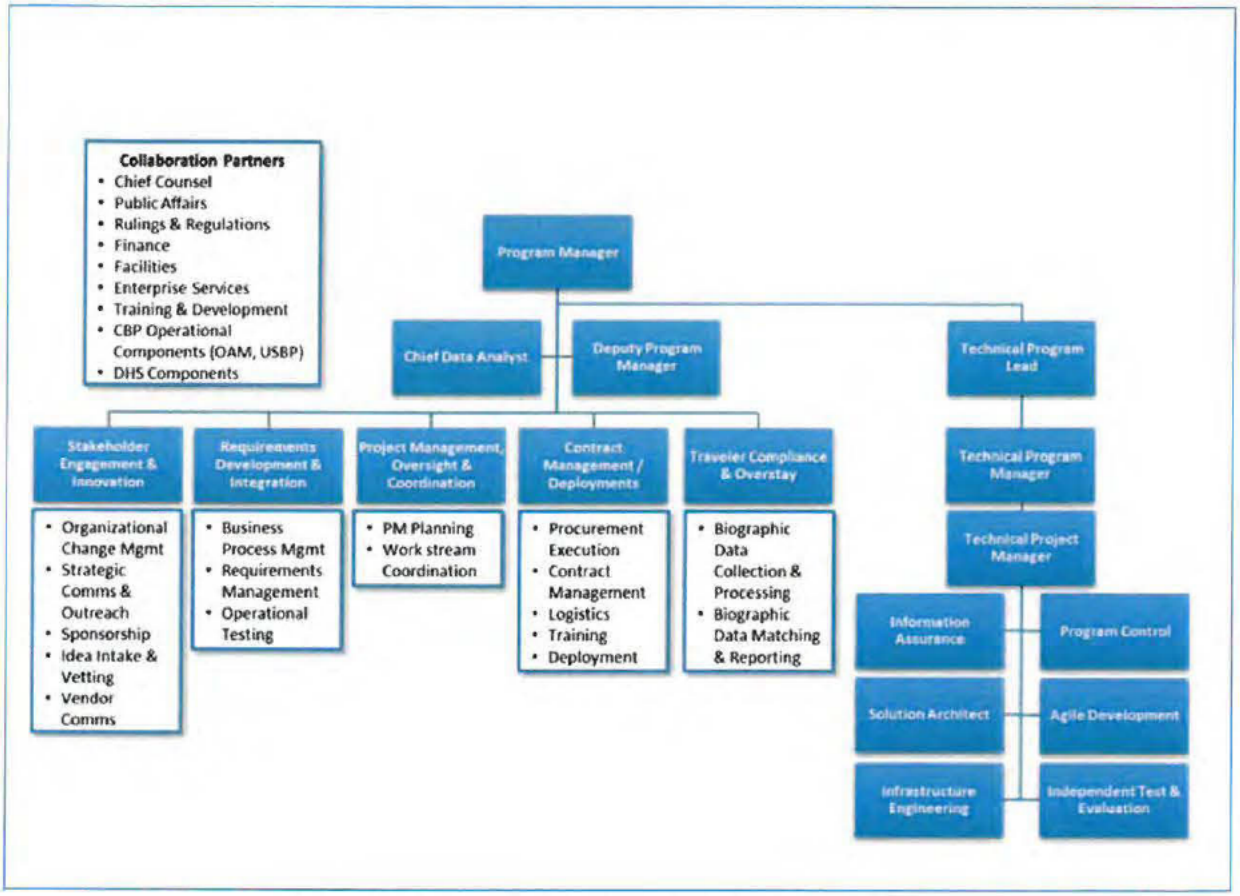


Figure 7 – Biometric Entry/Exit Organization Chart

2.6 Potential Impacts

The following are potential impacts to operations with implementation of a biometric exit solution:

- Updated outbound policies, processes, and directives will need to be developed to detail CBP enforcement response to watch list hits on exit.
- New policies, processes, and directives will need to be coordinated with other stakeholders to respond to travelers whose exit cannot be biometrically confirmed. Common exceptions are failure to capture a live image and failure to match an image in the gallery.
- A strong public outreach and communication plan will need to be implemented for interfacing with the traveling public and third party stakeholders.
- In the event of a false accept occurring during biometric matching (where a traveler is incorrectly identified by through biometrics as someone else), the data integrity of the system and the resulting biometrically confirmed crossing records are negatively impacted.

- CBPO staffing requirements will need to align with the expected workload generated by the Biometric Exit program to minimize impact to scheduled departures.
- Specifically for land travelers and travelers from visa waiver program (VWP) countries, the initial volume of travelers without biometrics on file or with poor quality biometrics on file will impact the throughput of Biometric Exit until CBP enrolls biometrics for a significant amount of these repeating travelers.
- In the event TVS is operating in a limited capacity or is unavailable, stakeholders will require guidance for processing travelers. In complete absence of the service, departures will be biographically confirmed. High availability requirements will minimize service disruptions.

3 Scenarios

3.1 Scenario Overview

This section identifies biometric entry-exit scenarios illustrating how travelers, stakeholders, and CBP will interact with the solution. They describe the operations and support capabilities necessary for successfully achieving mission objectives.

3.2 Mission Operations Scenarios

The following sub-sections identify the mission operations scenarios for biometric exit at air, land, and sea. The scenarios for air, land, and sea share a common approach following the biometric pathway concept but are adapted to the unique needs to each mode of travel.

3.2.1 Air Exit Pre-boarding Scenario (Optional)

This scenario represents the process governing the biometric pathway concept at check-in, bag drop, and at the TSA security checkpoint. This scenario is an optional capability for stakeholders who elect to utilize biometric matching services provided by CBP prior to boarding to streamline their processes. At each of these steps in the air travel process, TVS will provide biometrically confirmed identity information to the stakeholder, providing an enhanced and seamless process for the traveler to present their identity.

Initial Condition: Airline traveler manifest created for departing international flight.

Final Condition: All exiting U.S. citizen and non-U.S. citizen air travelers between the ages of 14 and 79 are verified against biometric and biographic information and are able to proceed to boarding gate using biometrics as an alternative to presenting travel documents and a boarding pass. Any travelers with associated watchlist information or flags are interdicted following normal CBP operating procedures.

1. Airline traveler manifest for exiting international flight transmitted to CBP through APIS.
2. CBP creates a small, temporary, targeted biometric gallery based on CBP and other government source biometric holdings that is specific to the airline's transmitted manifest for all U.S. citizen and non-U.S. citizen air travelers between the ages of 14 and 79.
3. Traveler photograph captured by stakeholder upon flight check-in, baggage drop, and/or TSA security checkpoint.
4. Airline or TSA captured biometrics transmitted to CBP.
5. CBP performs matching and automated analysis between stakeholder-captured photograph and temporary manifest-specific biometric gallery while not impeding the flow of travelers through check-in, baggage drop, or security checkpoint. [See *Excursion 3 – Watch List Hit*]

6. CBP provides response to stakeholder (airline, TSA, or both) with traveler's biometrically confirmed identity and authorization to proceed. [*See Excursion 1 – Facial Recognition No-Match*]
7. Traveler proceeds without presenting travel documents or boarding pass.

3.2.1.1 Excursion 1 – Secondary Biometric Match (Optional Future Capability)

1. CBP response indicates that traveler's facial biometrics cannot be matched to existing biometric records.
2. Stakeholders may elect to provide fingerprints as a secondary biometric.
3. CBP performs matching and automated analysis.
4. Traveler identity confirmed by fingerprint matching. Traveler facial image enrolled in CBP biometric database. [*See Excursion 2 – No Biometric Match*]
5. Traveler proceeds without presenting travel documents or boarding pass.

3.2.1.2 Excursion 2 – No Biometric Match

1. CBP response indicates that traveler's biometrics cannot be matched to existing records.
2. Stakeholders follow existing procedures using travel documents and boarding pass.

3.2.1.3 Excursion 3 – Watch List Hit

1. CBP analysis indicates that a traveler biometrically identified has associated watch list information or flags.
2. CBP officer is notified on a work issued mobile device that a traveler has been identified with associated watchlist information and/or flags, the location of the biometric collection, and departing flight information for the associated traveler.
3. CBP interdicts the traveler with associated watchlist information or flags and executes the appropriate SOP.

3.2.2 Air Exit Boarding Scenario

This scenario represents the steps for utilizing the biometric pathway concept at boarding. Boarding is the final step in the air exit process and represents the point in time where the traveler commits to exiting the country. Biometric confirmation at the boarding gate is mandatory for CBP to achieve its mission. Stakeholders utilizing TVS are required to securely submit biometric images at the boarding gate so that CBP can biometrically confirm the exit. The following steps identify the air exit boarding scenario:

Initial Condition: Airline traveler manifest created for departing international flight.

Final Condition: All exiting U.S. citizen and non-U.S. citizen air travelers between the ages of 14 and 79 are verified against biometric and biographic information. In-scope, non-U.S. citizen travelers are recorded as completing a biometrically confirmed border crossing in OBIM IDENT/HART and indicated in TECS and ADIS.

1. Airline traveler manifest for exiting international flight transmitted to CBP through APIS.
2. CBP creates a small, temporary, targeted biometric gallery based on CBP and other government source biometric holdings that is specific to the airline's transmitted manifest for all U.S. citizen and non-U.S. citizen air travelers between the ages of 14 and 79.
3. Traveler photograph is captured when approaching the boarding gate.
4. Captured traveler photograph transmitted to TVS.
5. CBP performs matching and automated analysis between stakeholder-captured photograph and temporary manifest-specific biometric gallery while not impeding the flow of travelers through the boarding gate. [*See Excursion 2 – Watch List Hit*]
6. TVS provides response to the boarding gate attendant with traveler's biometrically confirmed identity and authorization to proceed. [*See Excursion 1 – Facial Recognition No-Match*]
7. CBP records in-scope, non-U.S. citizen traveler's egress through the boarding gate as a biometrically confirmed border crossing in OBIM IDENT/HART with indicators in TECS and ADIS.
8. Traveler proceeds through the gate and boards the aircraft.

3.2.2.1 Excursion 1 – Facial Recognition No-Match

1. TVS response indicates to the boarding gate attendant that traveler's facial biometrics cannot be matched to existing biometric records.
2. CBP Officers are notified on a work issued mobile device that a traveler failed to match to the manifest gallery. CBP Officer responds according to outbound policy and procedures.
3. Boarding gate agent follows CBP instructions for processing travelers who fail to be biometrically identified. The two operational outcomes are:
   a. Stakeholders follow existing procedures using travel documents and boarding pass; and,
   b. Traveler waits for a CBP Officer who will follow policies and procedures for processing travelers who are not biometrically identified.

3.2.2.2 Excursion 2 – Watch List Hit

1. CBP analysis indicates that a traveler biometrically identified has associated watch list information or flags.

2. CBP Officer is notified on a work issued mobile device that a traveler has been identified with associated watchlist information and/or flags, the location of the biometric collection, and departing flight information for the associated traveler.
3. CBP Officer interdicts the traveler with associated watchlist information or flags and executes the appropriate SOP.

3.2.3 Land Pedestrian Exit Scenario

This scenario represents the steps for implementing biometric exit for pedestrians at land based border crossings exiting the U.S. CBP will implement lessons learned from the initial deployment in the air environment to develop processes to support land based exit biometric identity verification operations. The following steps identify the land pedestrian exit scenario:

Initial Condition: Land Port of Entry (POE) pedestrian exit facility executing steady state operations. CBP creates and maintains a biometric gallery of frequent border crossers specific to the Land POE.

Final Condition: All exiting in-scope, non-U.S. citizen pedestrians verified against biometric and biographic information are recorded as completing a biometrically confirmed border crossing in OBIM IDENT/HART and indicated in TECS, and ADIS.

1. Non-U.S. citizen, in-scope pedestrians exiting the U.S. have photograph captured.
2. Pedestrian photograph securely submitted to TVS.
3. CBP performs matching and automated analysis between captured photograph and frequent crosser POE-specific biometric gallery.
4. TVS provides response to the POE CBP Officer with pedestrian's biometrically confirmed identity and authorization to proceed. [See Excursion 1 – Facial Recognition No-Match] [See Excursion 2 – Watch List Hit]
5. CBP records the in-scope, non-U.S. citizen pedestrian's egress through the border exit as a biometrically confirmed border crossing in OBIM IDENT/HART and indicates in TECS and ADIS.
6. Pedestrian proceeds through the border exit and leaves the U.S.

3.2.3.1 Excursion 1 – Facial Recognition No-Match

1. TVS response indicates to the POE CBP Officer that traveler's facial biometrics cannot be matched to existing POE frequent traveler biometric records.
2. CBP Officer executes SOP for alternate biometric/biographic verification of departing pedestrian.

3.2.3.2 *Excursion 2 – Watch List Hit*

1. CBP analysis indicates that a traveler biometrically identified has associated watch list information or flags.
2. CBP Officer is notified that a pedestrian has been identified with associated watchlist information and/or flags, the location of the biometric collection, and approximate pedestrian exit lane for the associated pedestrian.
3. CBPO interdicts the pedestrian with associated watchlist information or flags and executes the appropriate SOP.

3.2.4 Land Vehicle Exit Scenario

This scenario represents the steps for implementing biometric exit at land based border crossings exiting the U.S. via personally owned or commercial vehicle. Technical advancements for front-end biometric capture devices are required in order to capture live biometrics from travelers without exiting the vehicle. As technology improves, CBP will conduct tests to determine feasible approaches, both materiel and process based, for biometrically confirming vehicular passengers. An alternate scenario will be developed for commercial vehicle traffic exiting the Land Port of Entry (POE). The following steps identify a preliminary land vehicle exit scenario for the purposes of developing initial operational requirements with the understanding the approach may need to adapt to technical and environmental constraints for vehicular land exit:

Initial Condition: Land POE vehicle (commercial and POV) exit facility executing steady state operations. CBP biometric gallery of frequent vehicular border crossers specific to Land POE vehicular crossings is being used for biometric matching and analysis.

Final Condition: All exiting in-scope, non-U.S. citizen vehicle occupants verified against biometric and biographic information are recorded as completing a biometrically confirmed border crossing in OBIM IDENT/HART and indicated in TECS and ADIS.

1. The vehicular exit gate is positioned to prevent the approaching vehicle from crossing the border.
2. As the vehicle stops at the exit gate and arrives at the biometric capture device the vehicle license plate and photographs of all vehicle occupants are captured.
3. Vehicle occupant photographs are securely submitted to TVS.
4. CBP performs matching and automated analysis between captured biometrics and frequent vehicular crosser POE-specific biometric gallery.

5. TVS provides response to the POE CBPO with all vehicle occupants' biometrically confirmed identity and authorization to proceed. [*See Excursion 1 – Facial Recognition No-Match*] [*See Excursion 2 – Watch List Hit*]
6. CBP records the in-scope, non-U.S. citizen vehicle occupants' egress through the border exit as a biometrically confirmed border crossing in OBIM IDENT/HART with indicators in TECS and ADIS.
7. The vehicle exit gate opens to allow the vehicle to exit the U.S.
8. Vehicle and all cleared occupants proceed through the border exit gate, exiting the U.S.

3.2.4.1 Excursion 1 – Facial Recognition No-Match

1. The vehicle exit gate remains closed to prevent the vehicle from exiting the U.S.
2. CBP response indicates to the POE CBPO that the occupant's facial biometrics cannot be matched to existing biometric records.
3. CBP executes SOP for alternate biometric/biographic verification of departing vehicular occupant.

3.2.4.2 Excursion 2 – Watch List Hit

1. The vehicle exit gate remains closed to prevent the vehicle from exiting the U.S.
2. CBP analysis indicates that an occupant's facial biometrics match biometric records with associated watch list information or flags.
3. CBPO is notified on a work issued mobile device that a vehicle's occupant has been identified with associated watchlist information and/or flags, the location of the biometric collection, vehicle license plate, and exit lane for the associated occupant.
4. CBPO interdicts the vehicle and its occupant with associated watchlist information or flags, and executes the appropriate SOP.

3.2.5 Sea Exit Boarding Scenario

This scenario represents the steps for implementing biometric exit at embarkation of sea travelers exiting the U.S. This scenario does not apply to closed-loop sea travelers who both embark and debark in the U.S. The following steps identify the sea exit boarding scenario:

Initial Condition: Sea traveler manifest created for departing cruise.

Final Condition: All exiting in-scope, non-U.S. citizen sea travelers verified against biometric and biographic information are recorded as completing a biometrically confirmed border crossing in OBIM IDENT/HART and indicated in TECS and ADIS.

1. Sea traveler manifest for exiting cruise transmitted to CBP through APIS.

2. CBP creates a small, temporary, targeted biometric gallery based on CBP and other government source biometric holdings that is specific to the cruise lines-transmitted manifest for all U.S. citizen and non-U.S. citizen sea travelers between the ages of 14 and 79.
3. Traveler photograph is captured prior to embarkation.
4. Captured traveler photograph transmitted to TVS.
5. CBP performs matching and automated analysis between the stakeholder-captured photograph and temporary manifest-specific biometric gallery while not impeding the flow of travelers at the sea port. [*See Excursion 2 – Watch List Hit*]
6. CBP provides response to the sea port attendant with the traveler's biometrically confirmed identity and authorization to proceed. [*See Excursion 1 – Facial Recognition No-Match*]
7. CBP records the in-scope, non-U.S. citizen in-scope traveler's embarkation as a biometrically confirmed border crossing in OBIM IDENT/HART with indicators in TECS and ADIS.
8. Traveler proceeds to boards the ship.

3.2.5.1 Excursion 1 – Facial Recognition No-Match

1. TVS response indicates to the boarding gate attendant that traveler's facial biometrics cannot be matched to existing biometric records.
2. CBP Officers are notified on a work issued mobile device that a traveler failed to match to the manifest gallery. CBP Officer responds according to outbound policy and procedures.
3. Sea port attendant follows CBP instructions for processing travelers who fail to be biometrically identified. The two operational outcomes are:
   a. Stakeholders follow existing procedures using travel documents and tickets; and,
   b. Traveler waits for a CBP Officer who will follow policies and procedures for processing travelers who are not biometrically identified.

3.2.5.2 Excursion 2 – Watch List Hit

1. CBP analysis indicates that a biometrically-identified traveler has associated watch list information or flags.
2. CBP Officer is notified on a work issued mobile device that a traveler has been identified with associated watchlist information and/or flags, the location of the biometric collection, and departing cruise information for the associated traveler.
3. CBP Officer interdicts the traveler with associated watchlist information or flags and executes the appropriate SOP.

3.3 Mission Support Scenarios

Three mission support functions are critical to Biometric Entry-Exit's success: program guidance and oversight, operations and maintenance, and training. Detailed Mission Support scenarios for each of these areas will be developed as the end-to-end system design evolves. The scenarios will illustrate how each of the following functions will operate within the overall system design.

Program Management – The program office will provide the guidance and oversight of all mission support activities in the form of standards, reporting requirements and active monitoring of ongoing performance. The office will also budget and track mission support activities using the budgets and spend plans provided by all the critical support organizations and contracts. The program office will report out on ongoing operations, reliability and performance in accordance with approved standards and metrics.

Operations & Maintenance (O&M) - The functional requirements for O&M will ensure maximum, sustained operational availability of TVS. Using a two-pronged approach of regularly scheduled preventive maintenance, on a quarterly basis, and immediate response for corrective maintenance ensures that all systems and equipment will perform to the highest performance standards over their lifecycle preventing impacts to trade and travel. Detailed operations and maintenance approaches will be developed by OIT and implemented through the OIT and supporting contractors. These will be described in the O&M Plans for each capability as it is developed.

Training – CBP Officers will require training for how to respond to PAU hotlist notifications. The functional requirements for training include both formal and informal approaches for ensuring training is available to all CBP officers when and where it is needed. Formal training requirements include formal instruction, formal documentation and training materials and certification standards. Informal training requirements address the need to have available ongoing refresher information such as can be posted on the Web. Training requirements also include the ongoing assessment of a user's ability to use and support the systems and equipment in order to ensure that updated information is made readily available as needed.

Table 14 provides a matrix of mission support category and responsible organization to meet support requirements for planned scenarios.

Table 14 - Mission Support Scenario Matrix

		Scenarios		
Category	**Responsibility**	**Air**	**Biometric Match**	**Program Management**
Logistics Management	OneNet/NOC EDC	Backend tele-communications and	Logistics planning and acquisition to	All Program Management

		Scenarios		
Category	**Responsibility**	**Air**	**Biometric Match**	**Program Management**
	Entry-Exit Program	computer logistical support planning and management	meet backend computer support requirements	activities – budget finance, acquisitions, schedules, staff Requirements Management and performance tracking
Logistics Engineering	OneNet/NOC EDC Entry-Exit Program	Backend tele-communications and computer logistical support engineering and operations	Logistics engineering for data storage and transmission capacity to meet matching performance requirements	Design and execute program processes Requirements Management and performance tracking
Support and Test Equipment	OneNet/NOC EDC OIT	Test and Support strategy, approach and equipment to support telecommunications, computing and software development testing and maintenance support	Test models and equipment to ensure performance compliance	N/A
Supply and Distribution Management	OneNet/NOC EDC OIT	Manage service level operational capacities. Manage acquisition and use of biometric data collection devices	N/A	Monitor performance to ensure compliance
Technical Data	EDC OIT Entry-Exit Program	Store and manage data collections (crossing histories, etc.) for operational use and future analysis	Store and manage data collections (biometric matches and non-matches) for operational use and future analysis	Review and assess to update/refine requirements and operational processes

		Scenarios		
Category	**Responsibility**	**Air**	**Biometric Match**	**Program Management**
Information Technology	OneNet/EDC OIT Entry-Exit Program	Telecommunications support, computer processing support, software test / production capabilities support	Computer processing support, software test/production capabilities support	Monitor and Track requirements
Infrastructure	OFO Facilities Management (Ports of Entry, Federal Inspection Areas)	Redesign/modify FIS facilities in airports to meet processing requirements	N/A	Facility/processing requirements compliance tracking and monitoring
Manpower and Personnel	OIT Entry-Exit Program	Ensure sufficient staff required to support technical operations and maintenance Ensure sufficient officers and agents needed to support requirements	Ensure analytical staff support for biometric matching analysis	Determine level, cost to acquire and cost to maintain officers and agents to support entry-exit.
Training and Trainers	OIT Entry-Exit Program	Ensure training development and trained trainers for system training	Trained analysts to support biometric match analysis	Ensure operational (policy, procedures) trainers – train the trainers
Maintenance	OneNet/NOC/EDC OIT Entry-Exit Program	Maintain telecommunications and wireless support for all transactions Maintain required hardware and system software to meet performance requirements Maintain applications and system software	Maintain biometric match systems	Monitor and track performance requirements

3.3.1 Maintenance Support Scenario

This scenario represents the process governing maintenance activities in support of biometric entry-exit operations at Air, Land, and Sea Ports of Entry. It is intended to present the stepwise troubleshooting and repair activities when TVS sub-systems require maintenance activity. The scope of the mission support scenario is for all TVS data center components and front-end biometric capture devices that are owned and operated by CBP. Travel industry stakeholders who own and operate their own front-end capture devices that interface with TVS are responsible for mission support of those systems.

Initial Condition: TVS System functioning outside of normal operating parameters.

Final Condition: TVS System functioning within normal operating parameters.

1. The TVS System built-in-test (BIT) notifies the CBP maintenance facility that a sub-system is operating outside of normal parameters.
2. The TVS operator executes alternate SOP for verifying traveler identities while the TVS system is being repaired.
3. CBP maintenance personnel create a maintenance ticket and remotely log into the TVS system to request a detailed health and status report.
4. Based on the health and status report details, CBP maintenance personnel initiate troubleshooting procedures from a remote location.
5. Troubleshooting indicates that software has become corrupt and requires re-loading and configuration.
6. CBP maintenance personnel upload the new software and configure the system remotely.
7. After successful software repairs the TVS health and status report indicates that a hardware subsystem is also malfunctioning. The CBP maintenance supervisor determines that the problem cannot be resolved remotely.
8. CBP maintenance personnel are dispatched to the location where the hardware failure has occurred with replacement hardware.
9. CBP maintenance personnel replace the malfunctioning hardware.
10. The TVS System BIT indicates that the system is functioning within normal operating parameters.
11. CBP maintenance personnel close the maintenance ticket and inform the TVS operator that the system has been repaired.
12. The TVS operator resumes using the TVS System to biometrically verify traveler identity per SOP.

4 Functional Capabilities

4.1 Functional Capabilities Matrix

4.1.1 Mission Operations Matrix

Table 15 traces the biometric entry-exit functional capabilities back to the missions and needs they support.

Table 15 - Mission Operations Matrix

		CBP MISSION							
		Counter Terrorism and Transnational Crime		Advance Comprehensive Border Security and Management		Enabling Lawful Trade and Travel			Promote Organization Integration, Innovation, and Agility
	FUNCTIONAL CAPABILITY	Enhance Procedures and Partnerships	Increase Situational Awareness of Air, Land and Sea	Detect, Interdict, and Disrupt Illegal Cross-Border Activities	Conduct Outbound Enforcement and Interdiction of Travelers	Identify Travel Threats as Early as Possible	Reduce Costs for U.S. and Trade and Travel Communities	Expand Risk-Segmentation to Enable Low-Risk Travel	Advance CBP Mission Effectiveness
1	Build small, targeted, temporary, searchable biometric galleries of expected travelers					P		P	
2	Build PAU hotlist based upon actionable biometric watch list hits and probable EWISs	P	P	P	P				
3	Receive live biometric images and associated image descriptive data captured by stakeholders						P		
4	Use live image to search the biometric gallery to identify the traveler						P		
5	Notify CBP Officers of PAU hotlist hits		P	P	P				
6	Record biometrically confirmed departures in OBIM IDENT/HART and ADIS								P
7	Provide reports								P

4.1.2 Mission Support Matrix

Table 16, Mission Support Matrix[13], provides a crosswalk of the required functional capabilities to the mission support function that will be established and notes the primary "P" or support "S" function that each capability will require throughout the deployed lifecycle.

Table 16 - Mission Support Matrix

	MISSION SUPPORT MATRIX						
	Program Management		Operations & Maintenance				Training
FUNCTIONAL CAPABILITY	Program Planning and Budgeting Policy	Guidance, Support and Oversight (Standards and Reporting)	Front-end Biometric Devices	Port Infrastructure	Backend Applications	IT Infrastructure	Staff
1 Build small, targeted, temporary, searchable biometric galleries of expected travelers		S	P		P		
2 Build PAU hotlist based upon actionable biometric watch list hits and probable EWISs		S	S	S	P	S	
3 Receive live biometric images and associated image descriptive data captured by stakeholders		S		S	P	S	
4 Use live image to search the biometric gallery to identify the traveler		S	S	S	P	S	
5 Notify CBP Officers of PAU hotlist hits		S		S	P	S	P
6 Record biometrically confirmed departures in OBIM/ DENT/HART and ADIS		S		S	P	S	
7 Provide reports and monitor system performance	S	S	P	P	P	P	

[13] While this crosswalk is often expressed in terms of "support modes" when describing physical assets (boats, planes, etc.), Biometric Entry-Exit consists primarily of information systems capabilities that use enterprise assets (network, computers, port facilities) that are supported directly by owners of the asset (OIT, Facilities, Stakeholder), not the program.

5 CONOPS Development Team

Biometric Entry-Exit IPT Members		
Office of Field Operations, Program Manager, Entry/Exit PMO	(b) (6), (b) (7)(C)	
Office of Information & Technology, Deputy Assistant Commissioner		
OFO, Deputy Program Manager, EntryExit PMO		
OFO, Chief Data Analyst, Entry/Exit PMO		
OIT, Technical Lead, Targeting & Analysis Systems Program Directorate		
OFO/EXT – Director, Program Management & Shared Services		
OFO/EXT – Director, Entry/Exit Mission Integration		
OFO/EXT – Director, Entry/Exit Policy and Planning		
OFO/EXT – Director, Traveler Compliance Division		
OIT, Project Manager, Passenger Systems Program Directorate		
OFO/EXT – Program Manager, Acquisition		
OIT/PSPD – Acquisition SME		
OFO/EXT – Project Manager		
OFO/EXT – Project Manager		
OFO/EXT – Project Manager		
OFO/EXT – Project Manager		
OFO/EXT – Biometric SME		
OFO/EXT – Biometric SME		
OFO/EXT – Project Management Support		
OFO/EXT – Acquisition Management Support		
OFO/EXT – Acquisition Management Support		

6 Appendices

6.1 Acronyms

Acronym	Definition
ADIS	Arrival Departure Information System
APC	Automated Passport Control
APIS	Advance Passenger Information System
ATS	Automated Targeting System
BCI	Border Crossing Information
CAR	Capability Analysis Report
CBP	Customs and Border Protection
CEAC	Consular Electronic Application Center
CIS	Central Index System
CM	Configuration Management
CONOPS	Concept of Operations
CRE	Component Requirements Executive
CSIS	Consolidated Secondary Inspection System
DHS	Department of Homeland Security
DoS	Department of State
DOTmLPF-R/G/S	Doctrine, Organizations, Training, Materiel, Leadership, Personnel, and Facilities, plus Regulations/Grants/Standards
EDC	Enterprise Data Center
EID	Enforcement Integrated Database
EWI	Entry without Inspection
FIS	Federal Inspection Services
FY	Fiscal Year
GA	General Aviation
GES	Global Enrollment System
HART	Homeland Advanced Recognition Technology
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
INA	Immigration and Nationality Act
IRTPA	Intelligence Reform and Terrorism Prevention Act
IT	Information Technology
JRC	Joint Requirements Council

Acronym	Definition
LPR	License Plate Reader
MNS	Mission Need Statement
MSBM	Mission Support Business Model
NTC	National Targeting Center
O&M	Operations & Maintenance
OBIM	Office of Biometric Identity Management
OFO	Office of Field Operations
OIT	Office of Information and Technology
ORD	Operational Requirements Document
PAU	Passenger Analytical Unit
PII	Personally Identifiable Information
PL	Public Law
PMO	Project Management Office
PED	Pedestrian (application)
POE	Port of Entry
POV	Privately Owned Vehicle
SLA	Service Level Agreement
SORN	System of Record Notice
TCN	Third Country National
TSA	Transportation Security Administration
U.S.	United States
USC	United States Citizen
USCIS	U.S. Citizenship and Immigration Services
VPAIS	Vehicle Primary Application Integration Services
VWP	Visa Waiver Program

6.2 References

- 2014 Joint Preliminary Mission Need Statement on Biometrics
- DHS Biometric Strategic Framework: 2015-2025, June 9, 2015
- DHS Biometric Winter Study, March 2016
- Biometric Exit Vision White Paper (Final), December 1, 2016
- Biometric Exit Spend Plan (Final), January 3, 2017
- Biometric Entry-Exit Mission Need Statement (v1.0), February 1, 2017
- Biometric Entry-Exit Capability Analysis Report (v1.0), February 2, 2017
- Fiscal Year 2017 Biometric Entry-Exit Staffing Plan (v1.0), February 21, 2017
- Acquisition Decision Memorandum, February 16, 2017

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

Privacy Impact Assessment Update
for the
Automated Targeting System

DHS/CBP/PIA-006(e)

Contact Point
(b) (6), (b) (7)(C)
National Targeting Center
U.S. Customs and Border Protection
(b) (6), (b) (7)(C)

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

~~LAW ENFORCEMENT SENSITIVE / FOR OFFICIAL USE ONLY~~

~~THE ATTACHED MATERIALS CONTAIN INFORMATION THAT IS "LAW ENFORCEMENT SENSITIVE" AT THE DEPARTMENT OF HOMELAND SECURITY.~~

~~The portions highlighted below in red are law enforcement sensitive.~~

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

1.2.1 ATS Biometric Vetting Using Facial Recognition

Last updated December 12, 2019

On January 13, 2017, CBP issued ATS Addendum 1.2 to assess its "Facial Recognition Technology Update" that describes the process by which CBP will use ATS to search the FBI's NGI Interstate Photo System (IPS), which contains all photos received by the FBI with ten print criminal booking transactions. That process required CBP to send photographs to the FBI for matching, and the FBI then sent CBP possible matches for CBP to adjudicate.

CBP is conducting an update to ATS Addendum 1.2 because CBP has developed its own in-house facial recognition matching technology, the Traveler Verification Service (TVS),[1] currently used for identity verification and biometric entry and exit. This updated ATS Addendum 1.2.1 describes the process by which CBP will use the TVS technology to conduct facial recognition biometric vetting checks against certain populations in the same manner as existing biographic vetting checks.

Biometric Vetting using Facial Recognition and TVS Technology

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS) to facilitate legitimate trade and travel while managing the shared threat to the Homeland posed by individuals and cargo that may require additional scrutiny prior to entering or exiting the United States. Currently, ATS uses biographic identifiers and other selectors, such as name and date of birth, to assist in targeting and entity resolution[2] for individuals traveling or intending to travel to and from the United States. In addition to the biographic entity resolution capabilities used to identify matches to derogatory records, CBP intends to expand its analysis, targeting, and vetting capabilities by deploying biometric matching using facial recognition technology. This capability will allow CBP to enhance the identification of possible threats by leveraging facial recognition technology to identify biometric matches to derogatory records that are not identified through existing biographic targeting and entity resolution mechanisms.

Biometric Vetting v. Identity Verification

Biometric vetting using facial recognition is separate from the use of TVS for identity verification, by which travelers present themselves to CBP or an airline representative for a photograph immediately prior to entering or departing the United States. During biometric entry

[1] *See* DHS/CBP/PIA-056 Traveler Verification Service, *available at* www.dhs.gov/privacy.
[2] ATS uses entity resolution algorithms to connect disparate data sources under one view to understand possible entity matches and non-obvious relationships across multiple source systems.

and exit, TVS is currently used for *identity verification* purposes to confirm that the individual who attempted to enter or exit the United States at that particular time and location matches the travel document he or she is presenting for inspection.

Under the biometric vetting using facial recognition initiative, CBP will use the TVS technology to match photographs already accessible from existing ATS holdings and ATS interfaces and mirror the existing biographic vetting process. The types of photographs already accessible from existing holdings are photographs captured by CBP during previous entry inspections, photographs from U.S. passports and U.S. visas, immigration records, and photographs from prior DHS apprehensions and encounters.[3] As ATS performs its existing vetting and analysis process using biographic identifiers, it will also match those available photographs against available photographs associated with derogatory records, such as TECS lookout records, Terrorist Screening Data Base (TSDB) records, and outstanding wants and warrants.[4] CBP is not matching the facial images already accessible from existing ATS holdings and ATS interfaces against any state Department of Motor Vehicle (DMV) photographs. In instances in which biographic identifiers alone do not match to derogatory records but there is a match to derogatory photographs, CBP will conduct a manual review of the identified match to confirm whether the derogatory record is a true match to the individual based on the facial recognition technology. As part of the manual review, that individual then may be a subject of interest and the information will be stored in ATS as a Targeting Framework (ATS-TF) "event" for manual Officer review. This initiative will leverage TVS's facial recognition service, which relies on biometric templates also referred to as "galleries" generated from pre-existing photographs that ATS already maintains or accesses through existing ATS interfaces.

CBP will deploy biometric vetting using facial recognition in ATS for the following populations: (1) individuals seeking to enter or exit the United States whose names appear on a flight or vessel manifests, or voluntary manifests submitted by bus or rail manifest ("manifested travelers"); (2) individuals applying for CBP programs facilitating travel to the United States, and (3) subjects of interest who require additional research and analysis. CBP will match photographs for these three populations against a predetermined gallery of photographs associated with derogatory information. The process for biometric vetting using facial recognition and a description for all populations is outlined below.

---

[3] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. *See* Privacy Impact Assessment: Consular Consolidated Database, available at https://20012009.state.gov/documents/organization/93772.pdf. Other photos may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records.

[4] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy.

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

1. Manifested Travelers

ATS populates photographic galleries based on upcoming Advance Passenger Information (API) and/or Passenger Name Record (PNR)[5] information in the air and sea environments, which identify who is scheduled to travel; in the land environment bus and rail manifests voluntarily provided by carriers may be used to perform this function.[6] ATS uses the biographic information in the API or PNR to retrieve existing records in other ATS holdings and interfaces. If those holdings in ATS have an associated photograph (i.e., travel documents or encounters), that photograph will become part of the photographic gallery. The photographic gallery is then biometrically compared using facial recognition against a separate gallery of photographs that are associated with derogatory information, which include TECS Lookout Records, TSDB records received via the Watch List Service (WLS), and outstanding wants and warrants.[7] If a photograph from a travel document or encounter gallery is positively matched to the gallery of derogatory photographs, the associated derogatory information is presented to CBP personnel for further review and analysis. The manual process to determine if a derogatory record is a match to a traveler based on the facial recognition technology follows the same process as for biographic matches, using the totality of information available to the analyst. CBP will build galleries up to 24 hours prior to the scheduled departure for the manifested traveler population. These photo galleries for manifested travelers are then retained for 14 days (except for photo galleries of U.S. citizen travelers, which are purged upon the completion of arrival/departure processing) to permit CBP time to conduct further analysis.[8] While most determinations could be made in a shorter period, the 14 days may be necessary to collect additional information from other sources, such as Government agencies, to complete final vetting determinations, if necessary and appropriate. ATS may not have access to facial images for some travelers or travel applicants, such as for some first time Electronic System for Travel Authorization (ESTA) travelers or Canadian travelers. In such instances ATS will continue to only use biographic identifiers for matching to derogatory records.

[5] PNR information will only be used if there is no corresponding APIS record, and is limited to only retrieving the biographic information of the PNR record in order to search for associated photographs in ATS holdings and interfaces.

[6] See DHS/CBP/PIA-001 Advance Passenger Information System (APIS) *available at* www.dhs.gov/privacy.

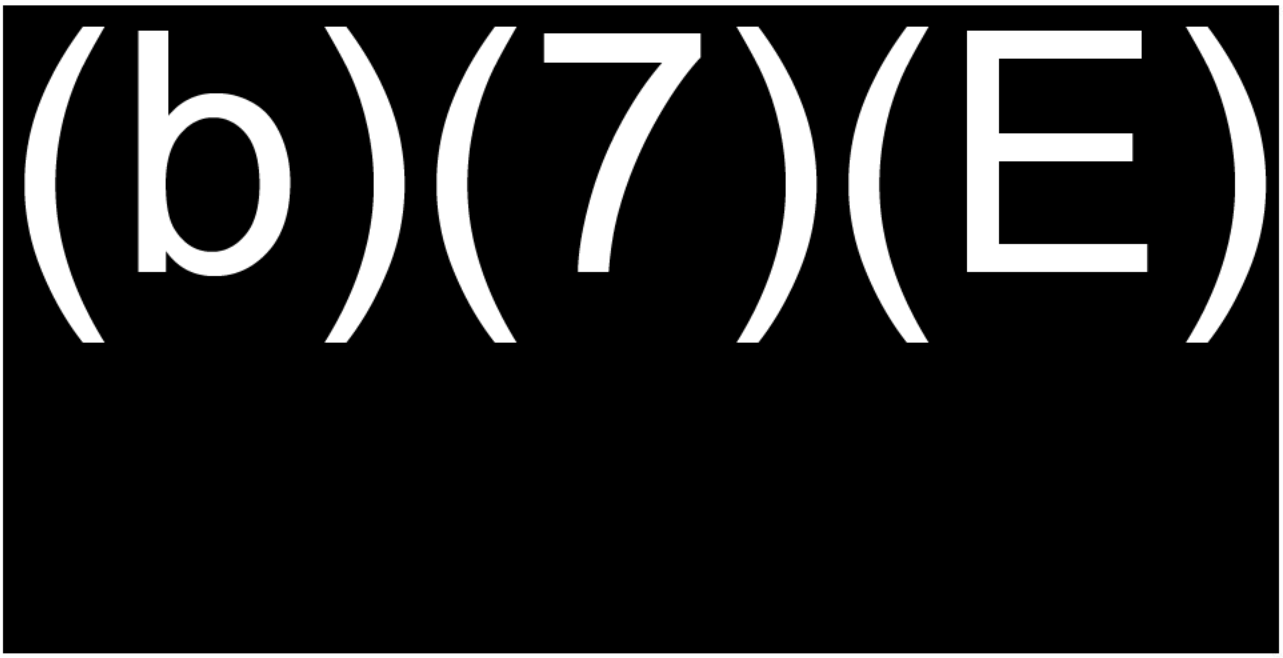
(b) (7)(E)

[8] CBP uses the facial images collected in the TVS to continually test and evaluate the accuracy of the camera technology and the algorithms. CBP retains the images of in-scope travelers for up to 14 days in order confirm travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

2. Travel Applicants

The same process described above will apply to vetting travel applications such as visas, the Electronic Visa Update System (EVUS), ESTA, and trusted traveler programs.[9] Biographics from those applications will be matched against biographics in ATS holdings and interfaces that also have an associated photograph. Those photographs will then be matched against the gallery of photographs that are associated to derogatory information. The galleries of photographs for vetting travel applications are built as new applications (such as visas, EVUS, ESTA, trusted traveler programs) are received by ATS. Any photographs associated with the applications are added to the associated photo galleries for those travel applications, to be compared against photographs from derogatory records. The photographs will be maintained in the gallery for the travel applications for the time period for which ATS is authorized to maintain the application data and associated photographs.



3. Research and Analysis for Subjects of Interest

In addition to the expanded targeting capabilities, CBP intends to use facial recognition technology to augment current search capabilities by allowing users of ATS to manually upload the photograph of a subject of interest into the federated query function to search ATS data holdings. This capability will aid ATS users in the identification of an individual who, for example, presents invalid documentation, or with identification in other encounters where biographic

[9] See DHS/CBP/PIA-002 Global Enrollment System (GES), DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA), and DHS/CBP/PIA-033 Electronic Visa Update System (EVUS) *available at* www.dhs.gov/privacy.

information alone cannot be easily matched. This capability is analogous to searching biographic data in ATS with the Super Query function, only now a user can enter a photograph into the Super Query function and the facial recognition technology will match that photograph to existing photographs in ATS holdings and interfaces. Additionally, CBP may receive from foreign or U.S. law enforcement partners photographs of individuals who are linked to possible illicit activity, which will be matched against derogatory records available in ATS.

(b)(7)(E)

Gallery of Photographs Associated with Derogatory Information

ATS aggregates Lookout Records from information that is associated with individuals who may be engaged in illicit activity, which may include photographs in addition to biographic identifiers. This information creates a gallery of derogatory information in ATS that is continually updated in real time. As ATS receives new derogatory records, if photographs are also part of the derogatory record, they are also added to the photo gallery. If the source derogatory record is updated to add or remove photographs, the associated photographs are also added to or removed from the photo gallery.

(b)(7)(E)

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

All previously identified SORNs remain in effect or are noted under the "Notice" section below.

Characterization of the Information

In order to properly evaluate travelers at the border, or those who intend to travel to the United States, CBP receives travel or application data and conducts vetting at the time of application submission, pre-departure or pre-arrival vetting for manifested travelers, or vetting at the time of arrival in the United States. In addition, CBP conducts research and analysis on available information to identify individuals who may need additional scrutiny. CBP uses this information to conduct checks against various derogatory records, such as TSDB records received via the WLS, TECS lookout records, wants and warrants entered by law enforcement officers, or ATS rules. Additionally, CBP Officers and United States Border Patrol (USBP) agents encounter and apprehend subjects who do not have valid travel documentation to enter the United States and conduct research to complete an individual inspection. The original point of collection for the data being used came directly from the traveler or from the traveler via the commercial carrier prior to entry and departure from the United States. There is no new collection of information by deploying facial recognition capabilities in ATS; rather, ATS targeting and entity resolution algorithms will leverage existing photographic images to perform matching in addition to biographic identifiers currently being used by ATS. Both biometric and biographic data located in ATS is derived from the source system through existing processes and described in the previously published PIAs.

Privacy Risk: Although no new information is being collected, there is a risk that the new technology being used for vetting may be inaccurate and generate false matches.

Mitigation: ATS will leverage the TVS facial recognition technology, for which CBP is continually testing and evaluating the accuracy of the matching algorithms. DHS personnel are also required to manually review and cross reference the records in ATS to improve the level of

confidence and reliability in matches made to derogatory information before any adjudication decision is made. In addition, DHS personnel will use all available information when making a decision and no adverse action will be taken from the results of facial recognition technology alone.

Uses of the Information

ATS will leverage photographs available via existing ATS holdings and interfaces and will provide a new method for identifying matches to derogatory records or other holdings during the vetting process. The facial images available through ATS include images for which ATS is the system of record (i.e., ATS-TF or Intelligence Records System-Next Generation (IRS-NG)),[10] or come from source systems of records that are either ingested into ATS or available via query services using ATS interfaces with systems such as TECS, WLS, IDENT, NCIC, the Consular Consolidated Database (CCD), and the Central Index System (CIS).[11] ATS will leverage facial recognition algorithms from the TVS application that are continually evaluated for accuracy in collaboration with DHS Science and Technology Directorate (S&T), Office of Biometric Identity Management (OBIM), and National Institute of Standards and Technology (NIST).

Once a facial image is available via ATS for both the subject of interest and the derogatory records that are in scope for analysis, targeting, and vetting, matches can be identified based on facial recognition technology. Additionally, during the analysis, targeting, and vetting process of a subject of interest, the ATS federated query capabilities will be augmented to use the facial recognition technology to match the photograph of a subject of interest with the photographs available through ATS holdings or ATS interfaces. This technology helps identify additional matching records that may assist CBP in identifying individuals or applicants who may need additional scrutiny.

CBP will conduct the same vetting process for matches to derogatory records made using facial recognition technology as matches made through existing entity resolution methods that currently use biographic identifiers. All matches via facial recognition will still require manual review and will follow the same process as the vetting of derogatory records identified through existing targeting methods in ATS. For example, a traveler who matches a derogatory record via

---

[10] See DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012.
[11] See DHS/ALL/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), DHS/ALL/PIA-027 Watchlist Service, DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), and DHS/USCIS/PIA-009 Central Index System: available at www.dhs.gov/privacy. Also see the Privacy Impact Assessment for the National Crime information center: *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/ncic-identity-theft, and the Privacy Impact Assessment for the Consular Consolidated Database: *available at* https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf.

facial recognition during pre-departure vetting may be sent to secondary inspection upon arrival at a U.S. port of entry for additional examination by a CBP officer. Based on the officer's examination, this may result in having his/her ESTA, EVUS, or trusted traveler application denied. Additionally, under certain scenarios during pre-departure vetting, CBP may recommend to the airline to deny boarding to an individual because the person is likely to be found inadmissible upon arrival at a U.S. port of entry. However, CBP will not deny entry or make a recommendation to the airline to deny boarding based on facial recognition technology alone, but rather will make that decision based on the totality of the information (such as previous encounters or Officer interview). This technology will also assist CBP in determining that the derogatory photograph does not match the traveler, thus facilitating travel or the granting of the travel application or trusted traveler application. For example, if a traveler seeking admission to the United States is identified as needing additional scrutiny based on facial recognition, CBP may send that traveler for a secondary inspection, and would conduct additional research about the traveler, verify the traveler's identity, interview the traveler, search the traveler's luggage, and based on all available information, make an admissibility determination.

CBP access controls will ensure ATS users will only be authorized to access the data they are provisioned to view through the ATS entitlement roles. CBP will create biometric templates of each photograph in order to secure the photographs for matching and storage. Biometric templates are strings of multiple numbers that represent specified images and facilitate facial recognition matching within a secure environment. These templates cannot be reverse engineered for viewing by external parties so if an unauthorized user were to view the template, it would not be visible as a facial image. The photographs that are sourced from ATS holdings and used to generate the templates are stored securely in the CBP computer systems and databases in which they originate, and are not transferred and hosted in the secure virtual cloud environment.

Privacy Risk: There is a risk that the facial recognition technology generates an inaccurate match on biometric data.

Mitigation: This risk is mitigated. If the facial recognition technology generates a match on biometric data, but there is no match on any biographic data associated with these photographs, CBP officers are trained to further analyze and review the totality of the data. If biometric data shows a match to a derogatory record, but does not match to the biographic data associated to that record, the CBP officer will manually review the records and conduct further analysis. No adverse action is taken based on facial recognition technology alone.

Privacy Risk: Authorized users of ATS could use their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors using facial images.

~~FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE~~

Mitigation: All ATS users must undergo privacy training and obtain approval from their supervisor and the ATS system owner before gaining access to ATS. ATS performs extensive auditing that records the search activities of all users. These audit logs may be reviewed, and any inappropriate use will be referred to the appropriate internal investigations office (such as the Office of Professional Responsibility, the Joint Intake Center, or others as required) for handling. The detection of inappropriate use will also result in the suspension of the user's access to ATS until the use can be investigated. The entire breadth of ATS auditing capabilities (previously discussed in detail in the ATS PIA) will be leveraged to monitor the usage of these capabilities.

Notice

There are no new collections associated with this program. ATS uses images available via ATS holdings or interfaces that are derived from other source systems. For images collected by CBP, the source system PIA and SORN provide notice of the original collection of the information, and CBP provides additional notice when possible through signage, Privacy Act statements, and with information on the CBP.gov website. Such information provides notice regarding CBP's authorities and purpose for the collection, but do not provide timely and specific notice with regard to this particular activity. The extent of notice given to individuals for the collection of the photographs is addressed in each source system PIA.

Privacy Risk: There is risk that travelers will not be aware of the fact that CBP is using facial recognition to vet them against derogatory information.

Mitigation: This risk is partially mitigated by this PIA, which provides public notice of the way CBP will use facial recognition to improve identification of individuals who pose a potential security concern or warrant additional scrutiny. However, due to the various sources and methods associated with the original collection of the information, CBP cannot reasonably provide timely notice regarding its use of facial recognition for biometric vetting.

Data Retention by the Project

To ensure data minimization while meeting law enforcement priorities, CBP will build galleries up to 24 hours prior to the scheduled departure for the manifested traveler population. These photo galleries for manifested travelers are then retained for 14 days (except for photo galleries of U.S. citizen travelers, which are purged upon the completion of arrival/departure processing) to permit CBP time to conduct further analysis to make a determination, while limiting the time photo galleries for manifested travelers are maintained to protect the privacy interests. While most determinations could be made in a shorter period, the 14 days may be necessary to

collect additional information from other sources, such as Government agencies, to complete final vetting determinations, if necessary and appropriate. The original photos are still to be maintained under the system of record, or the copy of the data propagated to ATS, and are accessible for generating photo galleries for new manifests.

The photos associated with travel applications, photos associated with derogatory information, photos of travelers that have matched the photo galleries associated with derogatory information, and the photo galleries for travelers who are manually vetted through ATS are maintained in the system in accordance with the source system retention policy. ATS collects some photographs directly and derives other photographs from various source systems. To the extent information is collected from other systems, data is retained in accordance with the records retention requirements of those systems.

If CBP creates a record in ATS-TF or IRS-NG as part of any of the analysis, targeting, or vetting processes, any images associated with the subject of interest will be maintained in the ATS-TF or IRS-NG and may be available via the Analytical Framework for Intelligence. Records in ATS follow the NARA retention schedule as outlined in the ATS SORN.

Privacy Risk: There is a risk that CBP may retain facial images in the gallery for longer than is necessary.

Mitigation: This risk is mitigated. All facial images used for this initiative is already stored in ATS in accordance with the records retention requirements for the source system of that biometric. For images that are part of the gallery building process, U.S citizen images are deleted once the individual arrives or departs a port of entry and all other images are deleted after 14 days.

Information Sharing

CBP may share information that originates from a system of record with federal, state, local, and foreign authorities consistent with the Privacy Act and the relevant SORN, including for law enforcement, judicial proceedings, and other lawful purposes. Since this technology will be used to identify matches to derogatory records that may not be otherwise identified through current methods, CBP may need to share the information with the record owner to enhance or correct the source record and support better matching by other agencies. For example, if a traveler is matched to a TSDB record using facial images, but not by the biographic information associated with photograph, CBP would notify and enhance the source TSDB record with the new facial image from the traveler.

Non-CBP owned records available in ATS are accessed in accordance with existing information sharing agreements. Each agreement specifies the arrangement to use the data for in-

scope analysis, targeting, and vetting and does not place limitations on analysis, targeting and vetting using facial recognition technology.

Privacy Risk: Information related to the matches generated by the facial recognition capability may be shared under inappropriate circumstances.

Mitigation: Absent any legal prohibitions, CBP may share information from ATS with other DHS or Component personnel who have an authorized purpose for accessing the information in performance of their duties, possess the requisite security clearance, and assure adequate safeguarding and protection of the information. In addition, CBP may share information external to DHS consistent with the Privacy Act and routine uses published in the source system SORNs, the ATS SORN, and consistent with DHS policy and existing MOUs, including setting forth the restrictions on and conditions of use; securing, storing, handling, and safeguarding requirements; and controls on further dissemination.

Redress

As with all the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[12] To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: There is a risk that CBP will not provide adequate redress to an individual who was improperly denied entry to the United States, referred for secondary inspection, or otherwise impacted by a false match based on facial recognition.

Mitigation: This risk is mitigated. ATS is using this technology for photographs that are already collected and stored in ATS. Procedures for individuals to gain access to data maintained in source systems that provide data ingested into ATS are covered by the respective SORNs for those source systems. Individuals may follow the procedures outlines in published PIAs and SORNs to gain access to their information stored in those systems. Persons who believe they have been adversely impacted by this technology may submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel

[12] DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012).

screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

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

Auditing and Accountability

ATS has role-based access. Only the users who are provisioned to the appropriate role based on need to know will be authorized to access the facial recognition capability. All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and responsibilities of each user. Access by users, managers, system administrators, developers, and others to the facial image data and facial recognition capability is defined in the same manner and employs profiles to tailor access to mission or operational functions similar to other ATS data and capability. ATS user roles are highly restricted and audited. Access is restricted in the form of role-based access, which is based on a demonstrated need to know. Facial image data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. All ATS users with access to ATS are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements. The same auditing and accountability privacy risks and mitigations apply and have been addressed in previous PIAs.