



U.S. Customs and
Border Protection

1300 Pennsylvania Avenue NW
Washington, DC 20229

October 30, 2020

SENT BY ELECTRONIC MAIL TO: agorski@aclu.org

Ashley Gorski
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004

Re: **20-cv-02213-NRB**

**American Civil Liberties Union and American Civil Liberties Foundation (ACLU) v
U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection
(CBP), Transportation Security Administration (TSA), and U.S. Immigration and
Customs Enforcement (ICE)
Fifth Interim Release for FOIA request CBP-2020-024672**

Dear Ms. Gorski:

This is our fifth interim response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP) submitted January 9, 2020, in which you requested the following:

1. *All memoranda of understanding, information-sharing agreements, business requirements, contracts, letters of commitment, and other agreements with airlines, airports, other countries, or other U.S. federal, state, or local authorities, concerning any aspect of TVS, including the processing or receipt of data collected or generated through TVS.*
2. *All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning:*
 - a. *The acquisition, processing, retention, or dissemination of data collected or generated through TVS, including biometric templates;*
 - b. *Access by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities to data collected or generated through TVS, including biometric templates;*
 - c. *Retention or dissemination by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities of data collected or generated through TVS, including biometric templates.*
3. *All memoranda, briefing materials, advisories, presentations, or formal or informal guidance related to the December 5, 2019 announcement that “There are no current plans to require U.S. Citizens to provide photographs upon entry and exit from the United States,” and that “CBP intends to have the planned regulatory action regarding U.S. citizens removed from the unified agenda next time it is published.”*

4. *All records, excluding informal email correspondence, concerning the efficacy or efficiency of facial recognition technology, as compared to other biometric and/or biographic methods, for identifying visa overstays, reporting visa overstays by country, or identifying individuals using fraudulent travel documents.*

5. *Statistics created on or after November 1, 2018, concerning “facial comparison matching performance,” including valid matches, invalid matches, valid non-matches, invalid non-matches, consequences for individuals identified as non-matches, and the aforementioned data broken own by demographics including race, ethnicity, skin pigmentation, gender, age, and/or country of origin.*

6. *“Summary reports” that “present the actual performance of TVS against its [Biometric Air Exit Key Performance Parameters] in production.”*

7. *All final evaluations, tests, audits, analyses, studies, or assessments by the DHS Science and Technology Directorate, DHS Office of Biometric Identity Management, or the National Institute of Standards and Technology, in connection with CBP, related to (i) the performance of algorithms in matching facial photographs, and/or (ii) the performance of facial recognition technologies developed by vendors. This request encompasses records concerning whether the algorithms or technologies perform differently based on flight route or an individual’s race, ethnicity, skin pigmentation, gender, age, and/or country of origin.*

8. *All records, excluding informal email correspondence, concerning CBP’s implementation of recommendations by the DHS Science and Technology Directorate to conduct an analysis of the risk of “false matches based on the demographics (age, country of origin, gender) of travelers on individual flights.”*

9. *All final reports, memoranda, or budgets concerning the cost of implementation of facial recognition technology or TVS as part of entry and exit procedures.*

10. *All records, excluding informal email correspondence, concerning future interoperability between the TSA’s biometric capabilities and “mission partner systems,” including CBP and DHS Office of Biometric Identity Management systems.*

11. *All policies, memoranda, formal or informal guidance, training materials, or briefing materials concerning the purported legal basis for CBP to possess data on the TSA’s behalf in the course of a traveler identity verification process.*

12. *All memoranda, briefing materials, advisories, presentations, formal or informal guidance, or analysis concerning whether airline or airport involvement in TVS complies with Illinois’s Biometric Information Privacy Act.*

For this production, CBP processed two hundred fifty eight (258) pages of documents in response to your request. CBP has determined that forty five (45) pages of records are withheld in full pursuant to Title 5 U.S.C. § 552 (b)(5) and one hundred eighty eight (188) pages may be released,

Ms. Ashley Gorski
October 30, 2020
Page 3

in full or in part with redactions pursuant to Title 5 U.S.C. § 552 (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). In addition, we determined that twenty-five (25) pages were not responsive to this request.

Information regarding the applicable exemptions and response can be found at the following link: <https://www.cbp.gov/document/guidance/exemption-definitions>. Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

If you have any questions regarding this release, please contact Assistant United States Attorney Jennifer Jude by email at Jennifer.Jude@usdoj.gov or 212-637-2663.

Please notate file number CBP-2020-024672 on any future correspondence to CBP related to this request.

Sincerely,



Jennifer R Davis
Subject Matter Expert
Freedom of Information Act (FOIA)
U.S. Customs and Border Protection

Enclosed: 189 pages

~~FOR OFFICIAL USE ONLY~~



**Interconnection Security Agreement between the
U.S. Department of Homeland Security
Customs and Border Protection (CBP)
and the
Buffalo and Fort Erie Public Bridge Authority
(PBA) via the
Redundant Trusted Internet Connection
DHS RTIC**

**Automated Commercial Environment (ACE)
and
Pre-Arrival Readiness Evaluation (PARE)**

Version 1.7

December 18, 2017

ISA-2017-04-124

~~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 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 the DHS OneNet RTIC, CBP ACE, and PBA PARE Network Disclosure Offices.~~

~~FOR OFFICIAL USE ONLY~~

DOCUMENT CHANGE HISTORY

Version	Date	Description / Author
1.0	Jan 23, 2017	(b) (7)(E)
1.1	March 8, 2017	(b) (7)(E)
1.2	April 21, 2017	(b) (7)(E)
1.3	April 26, 2017	(b) (7)(E)
1.4	May 2, 2017	(b) (7)(E)
1.5	Nov., 20,2017	(b) (7)(E)
1.6	Dec. 11, 2017	(b) (7)(E)
1.7	Dec 18, 2017	(b) (7)(E)

CONTENTS

1.0 PURPOSE.....2

1.1 Security Network Connectivity Policy 2

1.2 ISA Requirements for Types of System Interconnections..... 3

1.3 Scope..... 3

1.4 Points of Contact (POCs)..... 4

1.5 References..... 5

2.0 INTERCONNECTION JUSTIFICATION.....6

3.0 SECURITY CONSIDERATIONS6

3.1 General Information/Data Description 6

3.2 Physical Security and Environmental Controls 7

3.3 Data Sensitivity 7

3.4 Services Offered..... 8

3.5 Period of Operation..... 8

3.6 User Community 9

3.7 Information Exchange Security 9

3.8 Formal Security Policy 10

3.9 Incident Reporting 10

3.10 System Monitoring..... 11

3.11 Security Audit Trail Responsibility 11

3.12 Specific Equipment/Service Restrictions..... 11

3.13 Dial-Up/Remote Connectivity 11

3.14 Training and Awareness 12

3.15 Security Documentation..... 12

3.16 Change Control 12

4.0 TOPOLOGICAL DRAWING13

5.0 SIGNATORY AUTHORITY.....14

ATTACHMENT A: SYSTEM CONNECTION OVERVIEW.....1

1.0 PURPOSE

This new Interconnection Security Agreement (ISA) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for the protection and handling of unclassified information between the Customs and Border Protection (CBP) and Buffalo and Fort Erie Public Bridge Authority (PBA) through the DHS Redundant Trusted Internet Connection (RTIC). Any specific requirements of the three signatory organizations are also included.

CBP Headquarters and the CBP Buffalo Field Office, along with the PBA have deployed the PARE pilot program, an automated traffic management system for commercial vehicles entering the U.S. from Canada, to optimize traffic flow and reduce congestion on the Peace Bridge during a planned three-year bridge resurfacing project. (b) (7)(E)

1.1 Security Network Connectivity Policy

DHS Sensitive Systems Policy Directive 4300A establishes DHS policy for network connectivity. The DHS Sensitive Systems Handbook 4300A establishes information security procedures for the DHS components.

The section on network connectivity (Section 5.4.3) states:

- a. Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
- b. Interconnections between DHS and non-DHS systems shall be established only through the Trusted Internet Connection (TIC) and by approved Service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, Service Level Agreements (SLA) or Interconnection Security Agreement (ISA).
- c. Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in, "Preparation of Interconnection Security Agreements," Attachment N to the *DHS 4300A Sensitive Systems Handbook*.
- d. ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
- e. ISAs shall be reviewed and updated as needed as part of the annual Federal Information Security Modernization Act of 2014 (FISMA) self-assessment.
- f. Components may complete a master Interconnection Security Agreement (ISA) that includes all transitioning systems as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, security policies refers to the set of rules that controls a system's working environment, and not to DHS information security policy). ISAs shall be signed by the appropriate AO.

- g. Components shall document interconnections between their own and external (non-DHS) networks with an ISA for each connection.
- h. The DHS Chief Information Officer (CIO) shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO shall ensure that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.
- m. Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs.
- n. Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.

1.2 ISA Requirements for Types of System Interconnections

System interconnections may be characterized as either direct or networked. Direct connections are single purpose point-to-point connections that support only the two connected systems. Directly connected systems do not rely on another network for their connectivity or security and are physically and electronically isolated from other networks and systems. Networked systems connect via an intervening network that exists as a general support system, not a single-purpose connection. Systems that are connected via an encrypted tunnel, whether on HSDN (Homeland Security Data Network) or any other network, are considered networked systems.

For networked U.S. Government systems, the ISA must include the owner and AO (Authorizing Official) of the network as well as the owners of the applicable systems.

1.3 Scope

This new interconnection security agreement addresses the interconnection between CBP and PBA by way of the DHS RTIC extranet infrastructure. (b) (7)(E)

(b) (7)(E)

1.4 Points of Contact (POCs)

For all issues associated with this agreement, the established points of contact are as follows:

Table 1: Points of Contact

CBP	PBA	DHS OneNet Redundant Trusted Internet Connection
Authorizing Official: Philip A. Landfried Assistant Commissioner OIT (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	Authorizing Official: (b)(6), (b)(7)(C) Operations and Facilities Manager Buffalo and Fort Erie Public Bridge Authority	Authorizing Official (AO): James Flanagan Deputy CIO Ph(O): (b)(6) (b)(6)
System Owner: James H. Byram ACE System Owner Director, Cargo Systems Development (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	System Owner:	System Owner: (b)(6) Director, DHS RTIC Ph(O): (b)(6) (b)(6)
Information System Security Officer (ISSO): (b)(6), (b)(7)(C) ACE Information System Security Officer (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	ISSO:	DHS RTIC ISSO:
Information System Security Manager (ISSM): (b)(6), (b)(7)(C) Information System Security Manager (acting) (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	ISSM:	ISSM: (b)(6) Information System Security Manager Ph(O): (b)(6) (b)(6)
Chief Information Security Officer (CISO): Alma R. Cole Cyber Security Directorate (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	CISO:	CISO: (b)(6) DHS HQ CISO Ph(O): (b)(6) (b)(6) (b)(6)

Program Manager: (b)(6), (b)(7)(C) Cargo Systems Program Director (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)	Program Manager: (b)(6), (b)(7)(C) Operations and Facilities Manager Buffalo and Fort Erie Public Bridge Authority	Program Manager: Brian Ogle Director, DHS RTIC Ph(O): (b)(6) (b)(6)
--	--	--

1.5 References

The documents that served as the primary source for this ISA are the two following National Institute of Standards and Technology (NIST) Special Publications, as well as the IT Security Policy Handbooks Guides, and Manuals of DHS, and the PBA.

DHS/CBP:

- NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*.
- NIST Information Technology Laborator (ITL) Bulletin, *Secure Interconnections for Information Technology Systems*.
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organization*.
- NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*.
- *DHS Sensitive Systems Policy Directive 4300A*.
- *DHS 4300A Sensitive Systems Handbook*.
- *DHS 4300A Sensitive Systems Handbook, Attachment N, Preparation of Interconnection Security Agreements*.
- *DHS 4300A Sensitive Systems Handbook, Attachment F, DHS, Incident Response*.

PBA:

- (b) (7)(E)
- (b) (7)(E)

2.0 INTERCONNECTION JUSTIFICATION

(b) (7)(E)

The expected benefit is to expedite and facilitate the end-to-end exchange and processing of data between the two or more network systems via secure communication and to reduce the overall WAN expenditures within the Department.

3.0 SECURITY CONSIDERATIONS

This section describes the security mechanisms in place to secure the connections between both systems. It outlines what the security considerations are and which organization is responsible for each. In some cases both organizations will share security responsibility.

3.1 General Information/Data Description

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b)(7)(E)

(b)(7)(E)

The DHS RTIC and the PBA Network shall protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems.

(b)(7)(E)

(b)(7)(E)

As defined by NIST Federal Information Processing Standard (FIPS) FIPS-199 and documented in the DHS Trusted Agent FISMA utilizing DHS FIPS-199 workbook.

3.2 Physical Security and Environmental Controls

(b)(7)(E)

3.3 Data Sensitivity

(b)(7)(E)

CBP ACE receives Commercially-Owned Vehicles license plate numbers from the PBA PARE system. Per CBP Privacy office review the license plate number is not considered Personally Identifiable Information (PII) data as the license number is connected with the vehicle and not a person. CBP ACE only uses the license plate number for specific information retrieval and logging the request. (b)(7)(E)

(b)(7)(E)
(b)(7)(E)
(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

- [REDACTED] (b)(7)(E)
[REDACTED] (b)(7)(E)
- [REDACTED] (b)(7)(E)
- [REDACTED] (b)(7)(E)
- [REDACTED] (b)(7)(E)
- [REDACTED] (b)(7)(E)

Table 2: FIPS 199 Security Categorization

System	Confidentiality	Integrity	Availability	Overall
CBP ACE	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)
PBA PARE	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)
DHS RTIC	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)

Security measures are in place to protect all data transiting the DHS RTIC Extranet and the DHS RTIC, as required by Office of Management and Budget (OMB). The drawings provided in this document identify the layered approach to security at the RTIC in section 4.0 of this document.

3.4 Services Offered

(b) (7) (E)

(b) (7) (E)

Services and ports that are needed to access the Department systems are listed in Attachment A (System Connection Overview. Ports, Protocols and Services).

3.5 Period of Operation

CBP and the PBA systems are operational 24 hours a day, 7 days a week.

3.6 User Community

All PARE system operators are PBA employees. (b)(7)(E)

(b)(7)(E)

3.7 Information Exchange Security

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

CBP ACE: The *DHS 4300A Sensitive Systems Handbook, Attachment G, Rules of Behavior* as specified by the DHS CISO applies to ACE RTIC and CBP ACE systems.

3.8 Formal Security Policy

DHS CBP Policy:

- *NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.*
- *DHS Sensitive Systems Policy Directive 4300A.*
- *DHS 4300A Sensitive Systems Handbook.*
- *DHS 4300A Sensitive Systems Handbook, Attachment D Type Accreditation.*
- *DHS 4300A Sensitive Systems Handbook, Attachment F, DHS, Incident Response.*
- *DHS 4300A Sensitive Systems Handbook, Attachment O, Vulnerability Assessment Program, Attachment O.*

PBA Policy:

- [REDACTED] (b) (7)(E)
- [REDACTED] (b) (7)(E)

3.9 Incident Reporting

The organization discovering a security incident will report it internally, in accordance with the organization's incident reporting procedures. Each organization will ensure that the other connecting organization is notified when security incidents may have affected the confidentiality, integrity or availability of the shared data or systems being accessed.

Table 3: Points of Contact for Incident Reporting

Contact Group	Phone/Email	Hours
DHS Network Operations Center (NOC) and Computer Incident Security Reporting Center (CSIRC)/Security Operations Center (SOC)	1-877-DHSINET or 1-877-347-1638 (Option 1 = NOC, Option 2 = SOC) DHS SOC Direct Line: [REDACTED] (b)(7)(E)	24 x 7 x 365
CBP	1-877-DHSINET or 1-877-347-1638 (Option 1 = NOC, Option 2 = SOC)	24 x 7 x 365

PBA PARE	(b)(6), IT Manager Buffalo & Fort Erie Public Bridge Authority Phone: (b)(6) Cell: (b)(6)	24 x 7 x 365
-----------------	---	--------------

3.10 System Monitoring

DHS RTIC IDS/IPS & Firewalls: Please contact the DHS SOC at 1-877-DHSINET or 1-877-347-1638 (Option 2). (b)(7)(E) for details on the DHS monitoring security vulnerabilities and compliance.

DHS RTIC performance and monitoring: Please contact the DHS SOC at 1-877-DHSINET or 1-877-347-1638. (b)(7)(E) for details on the DHS security monitoring tools:

Information provided upon request. The POC is CSIRC 1-877-DHSINET or 1-877-347-1638 (Option 2).

3.11 Security Audit Trail Responsibility

Both parties are responsible for auditing system security events and user activities involving the interconnection. Activities that will be recorded include:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

Given the voluminous nature of audit logs, the logs should be kept at a manageable size by setting logging levels appropriately. Automated tools will be used for scanning for anomalies, unusual patterns, and known attack signatures, and will be configured to alert a system administrator if a threat is detected. An experienced system administrator or security manager will periodically review the logs to detect patterns of suspicious activity that scanning tools may not recognize.

(b) (7)(E)

3.12 Specific Equipment/Service Restrictions

The use of specific prohibited or restricted Services, protocols, and ports listed in the DHS 4300A System Security Handbook require an approved waiver or exception agreement between the system AOs. Any additional interconnections to either system shall be documented in the appropriate security documentation and each party shall be notified of the new interconnections.

3.13 Dial-Up/Remote Connectivity

There is no remote dial-up to this system. All access is via network connectivity through secure connections.

3.14 Training and Awareness

Both parties will ensure that all individuals using the systems (i.e., CBP and PBA systems) have attended initial basic and annual refresher Computer Security Awareness and Training. Both parties will ensure that persons with significant security responsibilities for the systems receive annual role based training covering their specific areas of responsibility. This training should ensure that staff members know how to report suspicious or prohibited activities.

3.15 Security Documentation

The CBP has Security Authorization (SA) documentation (e.g., System Security Plan, Contingency Plan, Risk Assessments and Security Assessments, Interconnection Security Agreements, etc.) and all other security related documents will be made available for review and acceptance. SA documentation will be updated to reflect the establishment of this interconnection and whenever a significant system change occurs or at least annually. PBA documents the connection with CBP in the signed Memorandum of Understanding (MOU) between CBP and Buffalo and Fort Erie Public Bridge Authority regarding the implementation of the Pre-Arrival Traffic Management Program. This ISA shall be updated should any of the information contained within change. The following information, at a minimum will be maintained accurate within this ISA:

- Names of interconnected systems
- Organizations owning the other systems
- Type of interconnection
- Name and title of authorizing management officials (e.g. Chief Information Officer or Designated Authorizing Authority)
- Interaction among the systems
- Hardware inventory
- Software inventory
- Rules of Behavior

All future changes relating to the security architecture of either system will be updated within the corresponding security documents. The assigned Information System Security Officer(s) for each system shall provide the security documentation to the each organization upon request.

3.16 Change Control

Significant changes to the system architecture, documentation, or configurations will be reviewed, approved and documented in accordance with each organization's configuration/change control process. Each organization shall notify the other if a system change significantly changes the approved security posture of the system or introduces new significant residual risk to either system. Whenever significant changes are made at one or both organizations, e.g., through additional staff, Service, etc., this should be recorded as an addendum to the original ISA.

4.0 TOPOLOGICAL DRAWING

Diagram 1 - Interconnection Architecture Diagram: PBA PARE – CBP ACE



5.0 SIGNATORY AUTHORITY

This ISA is valid for three (3) years after the latest date on either signature listed below, if the technology documented herein does not change or if there are no other intervening requirements for updates. At that time it must be reviewed, updated, and reauthorized. The security controls for this interconnection will be reviewed at least annually or whenever a significant change occurs. Either party may terminate this agreement with thirty days advanced not PBA. Noncompliance on the part of either organization or its users or contractors with regards to security policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

CBP ACE AO Phillip A. Landfried Assistant Commissioner U.S. Customs and Border Protection	(b)(6), (b)(7)(C) 4/19/18
	Signature Date
PBA PARE AO Thomas A. Boyle Operations and Facilities Buffalo and Fort Erie Public Bridge Authority	(b)(6), (b)(7)(C) 6 FEB 2010
	Signature Date
DHS RTIC AO James Flanagan Executive Director Department of Homeland Security DHS RTIC Authorizing Official	
	Signature Date

ATTACHMENT A: SYSTEM CONNECTION OVERVIEW

DHS RTIC, CBP and PBA, allowed Ports, Protocols & Services

The following ports, protocols, and Services are allowed between DHS RTIC and CBP/ PBA, Network, Security Domains by default.

Ports, Protocols, and Services Chart	
	(b) (7)(E)
	(b) (7)(E)
	(b) (7)(E)
	(b) (7)(E)

CBP ACE

PBA PARE

(b)(7)(E)

Withheld in Full Pursuant to, (b)(5)

EXECUTIVE SUMMARY

Subject: ISA-2017-04-124: Interconnection Memorandum between U.S. Customs and Border Protection Automated Commercial Environment the Buffalo Peace Bridge and Fort Erie Public Bridge Authority

Issue:

Requests approval of this new Interconnection Security Agreement between the U.S. Customs and Border Protection (CBP) Automated Commercial Environment and Buffalo Peace Bridge and Fort Erie Public Bridge Authority to support the Pre-Arrival Readiness Evaluation pilot program.

Background:

CBP Headquarters and the CBP Buffalo Field Office, along with the PBA have deployed the Pre-Arrival Readiness Evaluation (PARE) pilot program, an automated traffic management system for commercial vehicles entering the U.S. from Canada, to optimize traffic flow and reduce congestion on the Peace Bridge during a planned three-year bridge resurfacing project.

Recommendation:

(b)(5)

Submitted by: Alma R. Cole
Date: 01/03/2018
Point of Contact: (b)(6), (b)(7)(C)
Telephone: (b)(6), (b)(7)(C)

FOR OFFICIAL USE ONLY



Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies

Report to Congress



Homeland
Security

U.S. Department of Homeland Security

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.



Homeland
Security

August 30, 2019

Message from the Assistant Secretary for Legislative Affairs

I am pleased to present the following report, "Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies," which has been prepared by the Transportation Security Administration (TSA) and the U.S. Customs and Border Protection (CBP). This report is required by Section 1919 of the *FAA Reauthorization Act of 2018* (P.L. 115-254), signed into law on October 5, 2018.

The report describes CBP and TSA's development and implementation of biometric technology pilots. It includes assessments on the operational and security impact of biometric technology; potential effects on privacy with the expanded use of biometric technologies methods to mitigate privacy risks; methods to analyze and address matching performance errors; and special assessments on the biometric entry-exit program.

This report is being provided to the following Members of Congress:

The Honorable Roger Wicker
Chairman, Senate Committee on Commerce, Science, & Transportation

The Honorable Maria Cantwell
Ranking Member, Senate Committee on Commerce, Science, & Transportation

The Honorable Ron Johnson
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary C. Peters
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Bennie G. Thompson
Chairman, House Committee on Homeland Security

i

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.

The Honorable Mike Rogers
Ranking Member, House Committee on Homeland Security

Please do not hesitate to contact us at (202) 447- 5890 if we may be of further assistance.

Respectfully,



CHRISTINE M. CICCONE
Assistant Secretary for Legislative Affairs

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.

Executive Summary

TSA, CBP, travelers, and travel industry partners recognize that identity and vetting are critically important elements in the air environment. Travelers are repeatedly asked to prove their identity within the travel continuum. Governments and industry partners must repeatedly verify travelers' asserted identity at check-in, bag-check, security checkpoint, and at departure. Projected increases in air travel volume, combined with current infrastructure and operational constraints, underscore the need to automate current processes. Facial biometric technology has potential to modernize and streamline the process without sacrificing safety and security by reducing the reliance on manual identity verification processes.

At the direction of Congress, CBP developed a pilot biometric entry-exit program to aid in the identity verification of travelers upon entry into and exit from the United States. CBP and the Department of Homeland Security (DHS) invested in developing an identity as a service solution (IDaaS) that uses facial comparison to automate manual identity verification. This solution is called the Traveler Verification Service (TVS). The biometric entry-exit program is carried out through a privacy-by-design model and firmly situated within the DHS Fair Information Practice Principles.¹

TVS offers a secure system that works quickly and reliably. It uses existing traveler data to build small galleries of faces associated with each departing flight and enables CBP and its partners such as TSA, select air carriers and airport authorities to simply take and submit a traveler's photo for identity verification. Live photos are compared against the correlating flight gallery² and TVS returns verification results in seconds. For travelers at the gate, this means the traveler's facial biometric can serve as a boarding pass. For industry partners, it can mean a convenient, efficient, and safe travel experience redefined by biometrics.

CBP established a rigorous process to review data associated with matching performance of biometric facial comparison. Although TVS true match rates can vary, CBP's analysis found a negligible effect in regards to biometric matching attributed to demographic variables. Further, because data privacy, protection, and mitigation of algorithmic or operational bias are prime concerns, CBP actively makes improvements while seeking to ensure there are no signs of bias,³

¹ See DHS Privacy Policy Directive 140-06, available at: <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles>.

² A pre-positioned "gallery" of traveler face templates is created using the biographic data from the airline manifest to retrieve the photos from government holdings, such as passports, visas, and previous entries.

³ CBP measures and evaluates true match and non-match rates, as well as false match and non-match rates to provide a comprehensive understanding of system effectiveness in alignment with its mission. CBP analyzes for

and engages in a robust public dialogue on appropriate standards. CBP also engages in outreach with privacy advocates, the National Institute of Standards and Technology (NIST), and U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) to monitor performance and progress.

While TSA is not evaluating the use of facial comparison for law enforcement purposes, it is assessing its use for traveler identity verification as part of its mission to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA is using CBP's TVS for international travelers in this assessment process. In October 2018, TSA published the *TSA Biometrics Roadmap for Aviation Security and the Passenger Experience*.⁴ The Biometrics Roadmap defines clear pathways to improve security, safeguard the Nation's transportation system, and accelerate the speed of action through smart investments and collaborative partnerships. In pursuing these goals, TSA seeks to use innovative collaboration concepts and solutions to enhance security effectiveness, improve operational efficiency, and yield a consistent, streamlined traveler experience. As it works to test the use of opt-in facial image collection and matching processes for additional populations, including TSA Pre✓[®] travelers and the general flying public, TSA is grounding its solutions in rigorous scientific study and analysis. TSA is committed to protecting traveler privacy as part of its biometrics effort, and as such, incorporates privacy considerations into each phase of biometric solution development.

Beginning in March 2017, CBP and TSA began evaluating the use of facial comparison at the security checkpoint through a series of multi-phased pilots. Early success on initial proof of concept testing in October 2018 encouraged TSA and CBP to explore the viability of expanded use of TVS at the checkpoint through data integration between TVS and TSA Secure Flight systems. Both agencies will continue to build on their efforts to evaluate the ways in which biometrics technology can improve the traveler experience. TSA and CBP are committed to enhancing security consistent with their homeland security missions and biometrics efforts, including facial comparison.

demographic biases in its biometric exit systems. No bias based on demographics has been statistically identified in its approach. However, operational and environmental conditions, such as lighting, show much greater correlation.

⁴ https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf



U.S. Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies

Table of Contents

Message from the Assistant Secretary	i
Executive Summary	iii
I. Legislative Language	1
II. Background	3
A. CBP’s Progress Toward a Biometric Exit System	3
B. CBP and TSA Partnership to Evaluate Biometrics at the Checkpoint	6
C. TSA’s Exploration of Biometrics	7
III. Operational and Security Impacts of Using Biometric Technology	11
A. CBP Operational and Security Impacts	11
B. TSA Operational and Security Impacts	13
IV. Potential Effects on Privacy and Mitigation Methods	19
A. CBP Approach to Mitigating Privacy Impacts	20
B. TSA Approach to Mitigating Privacy Impacts	22
V. TSA Methods to Analyze and Address Matching Performance Errors	26
VI. Performance Assessments and Audits of the Biometric Entry-Exit Program	29
A. Performance Assessments	29
Biometric Performance Analysis of CBP Systems	29
Ensuring Biometric Technologies Do Not Unduly Burden Travelers	30

v

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.

	Biometric Technology Impact on Travelers Overstaying Their Lawful Period of Admission	31
B.	Audits Performed	32
VII.	Conclusion	34
VIII.	Appendices	35
	Appendix A. DHS Fair Information Practice Principles	35
	Appendix B. Acronyms	36

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.

I. Legislative Language

This Report to Congress was compiled pursuant to Section 1919(c) of the *FAA Reauthorization Act of 2018* (P.L. 115-254), signed into law on October 5, 2018, which states in part:

(c) REPORT REQUIRED.—Not later than 270 days after the date of enactment of this Act, the Secretary shall submit to the appropriate committees of Congress, and to any Member of Congress upon the request of that Member, a report that includes specific assessments from the Administrator and the Commissioner of U.S. Customs and Border Protection with respect to the following:

- (1) The operational and security impact of using biometric technology to identify travelers.
- (2) The potential effects on privacy of the expansion of the use of biometric technology under paragraph (1), including methods proposed or implemented to mitigate any risks to privacy identified by the Administrator or the Commissioner related to the active or passive collection of biometric data.
- (3) Methods to analyze and address any matching performance errors related to race, gender, or age identified by the Administrator with respect to the use of biometric technology, including the deployment of facial comparison technology;
- (4) With respect to the biometric entry-exit program, the following:
 - (A) Assessments of— (i) the error rates, including the rates of false positives and false negatives, and accuracy of biometric technologies; (ii) the effects of biometric technologies, to ensure that such technologies do not unduly burden categories of travelers, such as a certain race, gender, or nationality; (iii) the extent to which and how biometric technologies could address instances of travelers to the United States overstaying their visas, including— (I) an estimate of how often biometric matches are contained in an existing database; (II) an estimate of the rate at which travelers using fraudulent credentials identifications are accurately rejected; and (III) an assessment of what percentage of the detection of fraudulent identifications could have been accomplished using conventional methods; (iv) the effects on privacy of the use of biometric technologies, including methods to mitigate any risks to privacy identified by the Administrator or the Commissioner of U.S. Customs and Border Protection related to the active or passive collection of biometric data; and (v) the number of individuals who stay in the United States after the expiration of their visas each year.
 - (B) A description of— (i) all audits performed to assess— (I) error rates in the use of biometric technologies; or (II) whether the use of biometric technologies and error rates in the use of such technologies disproportionately affect a certain race, gender, or nationality; and (ii) the results of the audits described in clause (i).

- (C) A description of the process by which domestic travelers are able to opt-out of scanning using biometric technologies.
- (D) A description of— (i) what traveler data is collected through scanning using biometric technologies, what agencies have access to such data, and how long the agencies possess such data; (ii) specific actions that the Department and other relevant Federal departments and agencies take to safeguard such data; and (iii) a short-term goal for the prompt deletion of the data of individual United States citizens after such data is used to verify traveler identities.

II. Background

Biometrics are recognized as unique physical characteristics that can be used to identify a person. Physiological traits such as fingerprints, facial images, iris patterns, hand geometry, speech, and gait, are all examples of biometric indicators. Today, biometrics are commonly used to accurately identify a person or authenticate an individual's identity. The U.S. Department of Homeland Security (DHS) uses biometric information for a variety of mission purposes. For example, U.S. Customs and Border Protection (CBP) uses biometrics as part of its border security mission and under its mandate to establish and implement a biometric entry-exit system. As part of its mission to protect the Nation's transportation systems and to ensure freedom of movement for people and commerce, the Transportation Security Administration (TSA) is exploring the use of biometrics for identity verification for both traveler screening, and to enable access to airport sterile areas by airport workers.

Over the past decade, significant developments and improvements in biometrics technology have occurred. At the same time, the use of biometrics technology has also prompted concerns about accuracy, privacy, and security, among other issues. While CBP and TSA explore the use of biometrics consistent with their respective missions, they are mindful of those considerations as well as the need to build to and utilize enterprise biometric services offered through DHS's Office of Biometric Identity Management (OBIM).

A. CBP's Progress Toward a Biometric Exit System

CBP has used biometrics to verify the identities of foreign nationals entering the United States at air ports of entry since the mid-2000s. In recent years, it has also made significant progress towards achieving a biometric entry and exit solution mandated by federal statute and executive orders. Under existing laws⁵ and Executive Order 13780,⁶ CBP is required to implement measures to verify identities of travelers upon entry to and exit from the United States. After receiving the biometric entry-exit mission in 2013 and through the authorization of fee funds,⁷ CBP accelerated the implementation of a capability to biometrically verify the identities of travelers arriving and departing the United States by air while facilitating travel processes.

In 2017, after several successful biometric pilots, CBP began vetting the Traveler Verification Service (TVS), a facial image matching service that uses biographic data to retrieve all associated traveler facial images from DHS holdings and segment them into smaller, more manageable data sets,⁸ for use in the live environment. TVS uses the product of a fusion of

⁵ See, e.g., *Intelligence Reform and Terrorism Prevention Act of 2004* (Pub. L. No. 108-458, 118 Stat 3638 (2004)) and the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53, 121 Stat. 266 (2007)).

⁶ <https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreignterrorist-entry-into-the-united-states>

⁷ The *FY 2016 Consolidated Appropriations Act* (P.L. 114-113) funded the Biometric Entry-Exit Program through the authorization of up to \$1B in fee collections on H-1B and L-1 visa applications through FY 2025.

⁸ For example, by flight, by cruise, or by frequent border crossers.

biometric and biographic information, enabling the biometric data to be the key to verify the traveler identity with the advance biographic data. The matching service compares the traveler's live photo to source images such as the travel document, enabling CBP to confirm the entry and departure of in-scope,⁹ aliens. TVS was initially demonstrated at airports across the United States, as well as in the sea environment in 2017. CBP began piloting the capability at land ports of entry in the pedestrian environment in August 2018.

CBP's facial matching service is being leveraged to support biometric entry and exit processing for sea and land operations. Each travel mode offers unique challenges that require integrated solutions to mitigate any potential negative impacts to travel and trade. Biometric solutions must be thoroughly designed and tested to ensure that they are effective; compatible with expediting travel; can be integrated into existing infrastructure, systems, and processes; are not cost prohibitive, and do not put individuals' privacy at undue risk.

Air Entry and Exit

CBP envisions the facial matching service will significantly reduce the need to manually check paper travel documents by providing an automated process which can replace manual checks of travel document across the travel continuum. In 2017, CBP demonstrated TVS at eight international airports at boarding gates using CBP officers to process each traveler. CBP also partnered with JetBlue Airways, Delta Air Lines, British Airways, and Los Angeles International Airport (LAX) to evaluate biometric exit boarding integrated with stakeholder departure control systems. In Fiscal Year (FY) 2018, CBP's transformed entry process using facial comparison was reengineered and deployed in the air entry environment at 15 airports including four preclearance locations, with plans to expand further in 2019.

PROGRESS TO DATE

Processed more than 20 million travelers using facial comparison including:

- 10,749,134 arriving flights
- 3,422,909 departing flights
- 5,576,903 preclearance flights
- 600,728 flights through TSA checkpoints
- 250 cruise ships
- Biometrically confirmed over 17,840 foreign nationals who overstayed

Figure 1 Biometric Entry Exit Statistics (as of June 2019)

⁹ An "in-scope" traveler is any person who may be required by law to provide biometrics upon entry into the United States pursuant to 8 CFR 235.1(f)(ii), or upon exit from the United States pursuant to 8 CFR 215.8. "In-scope" travelers include any alien other than those specifically exempt as outlined in the CFR. Exempt aliens include: Canadian citizens under Section 101(a)(15)(B) of the Immigration and Nationality Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the date of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

Prior to departure, the TVS creates a pre-positioned “gallery” of traveler face templates using the biographic data from the airline manifest to retrieve the photos from government holdings, such as passports, visas, and previous entries. During boarding, the stakeholder system takes a picture of the traveler. The TVS compares the picture against the gallery and provides a biometric match result.

Due to the success of CBP’s stakeholder engagement strategy to date, CBP has received letters of commitment from 26 airports and airlines to begin implementation of biometric exit using CBP’s matching service. CBP is actively working with each committed partner to implement biometric exit solutions. In FY2018, biometric air exit started at nine airports and ended at 16 airports. Total in-scope travelers exiting the country processed started at 40,000 monthly and ended FY2018 with 157,000 monthly. These numbers continued to grow steadily during FY2019, growing 54% since the beginning of the calendar year, with 548,000 being processed in the month of April 2019.

By 2022, CBP’s goal is to deploy biometric exit to the top 20 airports, which account for more than 97 percent of departing commercial air travelers from the United States. CBP is actively working to expand stakeholder partnerships and adoption, prioritizing the highest volume of international airports and carriers to achieve the biometric air exit implementation goal. CBP continues efforts to consider innovative ways to utilize TVS with mobile phones, tablets and watches. CBP will look to expand partnerships with international airports and governments and to further expand capabilities in preclearance locations to continually improve security and facilitation of traveler processes.

Sea Environment

Leveraging the investment in TVS for the air environment, CBP is partnering with the cruise industry to modernize traveler and crew inspections by implementing facial matching technology in the sea environment. Preparations are underway to apply the use of facial comparison technology in the debarkation (arrival) and embarkation (departure) points at seaports. These improvements will enable increased security and enforcement as well as facilitate traveler inspections.

Today, five major cruise lines are engaged with CBP to develop facial biometric processing supported by the TVS for closed-loop cruises.¹⁰ Going forward, a focus on expanding integration with cruise partners will be implemented, focused initially on closed-loop cruises for debarkation. Through FY2020, CBP will seek to expand across closed-loop embarkation. Beyond FY2020, capabilities will be expanded to open-loop cruise routes.

Land Environment

¹⁰ A closed-loop cruise is a term that refers to a cruise itinerary which begins and ends at the same U.S. location. An open-loop cruise is one that begins and ends in different ports, either departing from or arriving in the United States.

The Land Biometric Exit strategy focuses on implementing an interim exit capability while simultaneously investigating innovative technologies to reach the long-term goal of a comprehensive exit solution. CBP is actively piloting capabilities at the land border in both the pedestrian and vehicle environments to determine the best long-term approach for a comprehensive biometric entry-exit capability. Since September 2018, 139 impostors were identified on entry using the TVS capability in a land pedestrian environment. Details on the challenges of implementing biometrics in the land border are detailed in section VI, and CBP's strategy to mitigate those challenges are in section IV.

In late 2017, CBP began the initial implementation of an interim land exit approach to provide a capability for CBP to report the final departure from the United States of third-country nationals at land ports of entry.¹¹ The third country nationals' capability is a short-term solution that leverages the biometric exit mobile platform from the air environment and allows compliant in-scope travelers a means to biometrically report departure. Since January 2018, more than 180 mobile devices have been deployed to 74 land border ports of entry to support this initiative. CBP personnel have deployed to more than 50 locations to provide training courses for the mobile app to support these deployments.

CBP will continue to evaluate concepts of operation and technologies in the land environment to determine the final approach. Solutions being evaluated leverage the underlying TVS architecture in both the pedestrian and vehicle environments.

B. CBP and TSA Partnership to Evaluate Biometrics at the Checkpoint

In March 2017, CBP and TSA began evaluating the use of facial comparison at the TSA checkpoint for identity verification. In April 2018, the TSA Administrator and CBP Commissioner signed a policy memorandum promoting a collaborative approach to the continued development and use of biometric technology at airports.

The goal of the partnership is to enhance security and promote effective use of resources. CBP and TSA established multi-phased pilots involving volunteer international travelers. The first phase at John F. Kennedy International Airport (JFK) began in October 2017 to collect data and validate the technology. In the second phase at LAX in August 2018 and Hartsfield-Jackson Atlanta International Airport (ATL) in November 2018, TSA used CBP's TVS to test biometrics for identity verification in an operational environment. In the third phase, CBP and TSA will explore data-sharing and integration between biometric and traveler vetting systems. The goal will be to create a consolidated traveler identity verification that meets the operational needs of both agencies. In 2019, CBP and TSA plan to continue working on the necessary technical integration and pilot planning activities. The results of the pilot will help inform the rollout plans at TSA checkpoints.

¹¹ DHS/CBP/PIA-026(a), *Biometric Exit Mobile Program* (June 29, 2018), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp026a-bemobile-june2018.pdf>.

C. TSA's Exploration of Biometrics

TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. The TSA Administrator's 2018-2026 Strategy¹² details the three strategic priorities that will guide the agency as it seeks to further enhance transportation security.

- **Improve security and safeguard the transportation system:** TSA will lead by example by strengthening operations through powerful and adaptable detection capabilities, intelligence-driven operations, and enhanced vetting.
- **Accelerate action:** TSA will build a culture of innovation that anticipates and rapidly counters the changing threats across the transportation system. TSA will develop its ability to make timely, data-driven decisions, and rapidly field innovative solutions.
- **Commit to our people:** TSA will foster a diverse, inclusive, and transparent work environment, establishing itself as a choice federal employer. TSA will use available tools and authorities to cultivate a skilled workforce equipped to meet the challenges of tomorrow.

Identity verification and traveler vetting are integral to TSA's multi-layered security processes and core security mission. The identity verification process ensures that the person seeking access to the airport sterile environment is the person who was vetted by TSA's Secure Flight against intelligence-driven watch lists, and receives the appropriate level of physical screening. Currently, TSA relies on a manual identity verification process through which Transportation Security Officers (TSOs) and, for checked baggage, airline employees, verify a traveler's identity by manually reviewing their boarding pass and a valid form of identification (ID). For photo ID documents, TSOs must visually confirm the photo on the document matches the traveler. Once a TSO confirms a traveler's identity, he/she direct the traveler to proceed to security screening based on their Secure Flight vetting status as it appears on the boarding pass. Automated facial recognition capabilities can play an important role, in increasing the effectiveness of this travel document checker (TDC) position at the checkpoint.

TSA is deploying Credential Authentication Technology (CAT) to increase security at checkpoints. CAT addresses ID fraud vulnerabilities by verifying the security features on a traveler's ID and boarding pass. CAT also provides automated access to real-time Secure Flight traveler vetting information at the checkpoint. In the future, biometrics will complement the capabilities CAT offers by enabling TSA to match the person's facial image against the facial image on file or on their ID.

In 2013, TSA established the TSA Pre✓[®] Application Program. Under this trusted traveler program, TSA conducts significant additional vetting of applicants; those individuals that TSA has determined are low risk are then eligible for expedited screening at participating U.S. airports. Members of the traveling public voluntarily pay a fee and provide their biographic and information and fingerprints to conduct the enrollment and vetting to check an applicant's criminal history, potential ties to terrorism, enrollment eligibility, and citizenship. As of September 2018, TSA has transitioned from single-factor biometric enrollment (fingerprints) to

¹² Available at: https://www.tsa.gov/sites/default/files/tsa_strategy.pdf.

multi-modal biometric enrollment (fingerprints and face), so that facial images can be used for identity verification.

In June 2017, TSA assessed, as a proof of concept, the use of biometric authentication technology to verify the identity of TSA Pre✓[®] travelers. As part of this proof of concept, TSA compared a fingerprint scanned using this technology with the fingerprint provided at the time of TSA Pre✓[®] enrollment. This proof of concept demonstrated the potential for biometrics to enhance security through increased assurance of traveler identity. It also underscored the need for additional work to explore other biometric technologies, such as facial images, and integrate those biometrics into airport checkpoint operations.

Additionally, in 2018, TSA conducted a three-week proof of concept at LAX using facial comparison to provide automated verification of identities at the TDC. This proof of concept was available to e-Passport¹³ holders who volunteered to test the technology. Travelers scanned their e-Passports to verify the name on the e-Passport matched the name on the traveler's boarding pass. If it matched, the system extracted the traveler's digital photo from the e-Passport chip. The traveler was then prompted to complete a photo capture with a facial comparison camera. Facial comparison technology compared the e-Passport photo to the real-time photo and prompted the e-Gate to open if they matched. After the e-Gate opened, the travelers proceeded to the TDC; those who did not match were directed to the TDC officer. All passengers were required to complete the standard TDC process for manual identity and travel document verification, regardless of the e-Gate biometric matching results.

Recognizing the need for TSA to take a more comprehensive approach to biometrics, Administrator David Pekoske championed the development of the Biometrics Roadmap,¹⁴ published in October 2018. The roadmap provides the following:

- Defines clear pathways to improve security, safeguard the Nation's transportation system, and accelerate the speed of action through smart investments and collaborative partnerships;
- Incorporates feedback gathered during more than 40 engagements with aviation security leaders from airlines, airports, and solution providers; and
- Includes feedback gathered from key government stakeholders, including TSA internal offices, DHS headquarters, and operational components.

¹³ E-Passports contain an electronic chip that holds the same information that is printed on the passport's data page including a digital photograph of the holder. See <https://www.dhs.gov/e-passports>.

¹⁴ Available at: https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

It also outlines four goals to achieve TSA's vision for biometrics.

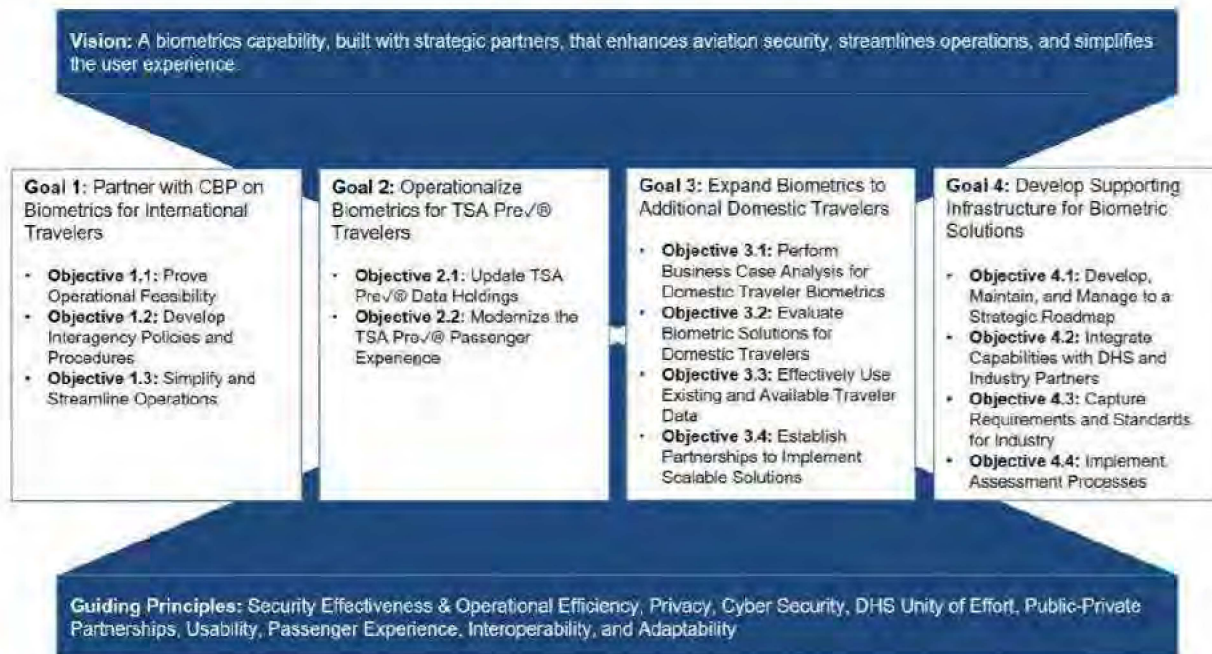


Figure 2 TSA's Vision, Goals, Objectives, and Principles for Checkpoint Biometrics

Goal 1: In partnering with CBP on biometric technology pilots, TSA is exploring the feasibility of applying biometric solutions at the TSA checkpoint. While CBP and TSA mission requirements differ in some regards, CBP's biometric air exit program offers the opportunity to conduct joint operational pilot projects, collect data, refine solutions, and exchange data. TSA's partnership with CBP will also enable TSA to identify and examine technical, legal, and regulatory issues before broader deployment.

Goal 2: To further implement biometrics for TSA Pre✓®, TSA continues enhancing the trusted traveler experience for TSA Pre✓® travelers. As of September 2018, TSA is capturing photos for those who renew in person or who are enrolling for the first time in the TSA Pre✓® Application Program.

Goal 3: TSA will explore opt-in biometric solutions for additional travelers beyond international outbound and trusted travelers. An assessment of the appropriate authorities, privacy issues, and potential risks and benefits as it explores ways to improve the screening experience for standard (non-TSA Pre✓®) domestic travelers will be conducted. As TSA explores biometric solutions for additional travelers, it will conduct pilot projects and seek input from a diverse group of stakeholders. Additionally, TSA will continue to partner with DHS and interagency partners, including DHS Science and Technology (S&T) Directorate, and OBIM, as well as CBP, and the DHS Office of Privacy and DHS Office of Civil Rights and Civil Liberties, to evaluate biometric solutions for domestic travelers.

Goal 4: TSA will develop supporting infrastructure for biometric solutions that align with legal and policy authorities. TSA's biometrics efforts will also align with the DHS-wide transition to enterprise biometric services offered through OBIM's Homeland Advanced Recognition Technology (HART) system. Common standards will also allow TSA to establish assessment processes, making it possible to quickly evaluate security procedure changes, assess cybersecurity posture, develop qualified product and service lists, and implement audits and controls to ensure operations adhere to applicable laws, policies, and compliance authorities.

III. Operational and Security Impacts of Using Biometric Technology

Recognizing the important role that biometric technology can play in enhancing security and improving operations, CBP and TSA are methodically studying the impact of these technologies through a number of pilots and demonstrations. Though the operational and security factors that are driving the use of biometric technologies are distinct for both agencies, CBP and TSA's assessments are helping to refine biometric solutions and biometrics efforts throughout DHS.

On an average day, CBP processes more than one million travelers arriving at air, sea, and land ports of entry. Innovative technologies are being used to enhance a wide range of its operational capabilities. The use of biometrics, specifically facial comparison technology, assists CBP in confirming the departure of non-U.S. citizens and facilitates future processing at entry and exit. Through CBP's development of biometrics at entry-exit, it has found that biometrics are an effective tool in combatting the use of stolen and fraudulent travel and identity documents. The goal is to ultimately enhance identity verification while facilitating a more secure travel experience.

A. CBP Operational and Security Impacts

In addition to the responsibilities referenced in Section II B, CBP has the ongoing mission to inspect all incoming and departing travelers and conveyances to determine admissibility to the United States and enforce and administer U.S. immigration laws.

A key aspect of effective enforcement is the ability to discern individuals who are lawfully present in the United States from those who have violated their terms of admission. An effective immigration system requires an end-to-end process that collects exit data and matches that to entry data. Without exit data, there is no meaningful way to determine whether foreign nationals have overstayed their periods of admission.

Biometric data, when used with biographic data, allows CBP to confirm with greater assurance a traveler's true identity, ensuring the traveler matches the biographic identity that has been vetted through DHS databases. 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 implement a biometric entry-exit solution that is both operationally feasible and realistic, CBP established key parameters based on existing operational constraints and infrastructure limitations.

CBP's Key Strategic Parameters Table 1

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 traveler behavior	Leverage traveler behaviors and expectations that require minimal new or unexpected steps for travelers.
Leverage existing data and IT infrastructure	Leverage existing traveler data, such as passport and visa information, and leverage existing government IT infrastructure as much as possible.
Utilize existing DHS enterprise biometric services, capabilities, and investments	Leverage and integrate with DHS Enterprise Services for shared biometric matching capabilities.

For the initial implementation of biometric exit solutions in the air environment, CBP is working 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. The strategic benefits are described in the following table:

CBP Strategic Benefits Table 2

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.
A positive impact on inbound security and throughput	Enhanced inbound security and more efficient throughput.
Improved traveler experience	An overall enhanced traveler experience.
Improved data integrity	Utilize DHS enterprise biometric repositories provided to ensure accurate biometric identity records.
Enhanced visa overstay enforcement	Support the ID and tracking of visa overstays by closing information gaps associated with current exit reporting capabilities allowing for improved enforcement action.

CBP is transforming the way the agency identifies 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 and automated traveler movement. CBP will continue to increase security by using a live facial biometric to match the traveler to advance traveler information, while also checking any existing fingerprints on file against the biometric watch list, which decreases dependency on less reliable paper travel documents, such as passports and visas. New facial comparison processes will enhance CBP's biometric capabilities alongside of the existing fingerprint processes.

CBP is partnering with the air travel industry and TSA to deploy a biometric air entry-exit solution that improves and streamlines the overall traveler experience. The four primary goals of this large-scale transformation is 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, as well as the collection of fingerprints;
- **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.

B. TSA Operational and Security Impacts

For TSA, biometrics can provide important benefits in air travel. TSA experienced a milestone year in 2018, screening a record setting 813.8 million travelers.¹⁵ This amounts to more than 2 million travelers per day. TSA is already on track to exceed this in 2019. Like TSA, airlines, airports, and security regulators around the globe are faced with an ever-rising volume of air travelers to screen. In light of rising air travel volume and operational constraints, TSA must look to innovative technologies, like biometrics, to enhance security and efficiency while improving the traveler experience.

¹⁵ <https://www.tsa.gov/blog/2019/02/07/tsa-year-review-record-setting-2018>

TSA evaluates potential changes to its aviation security programs and technology solutions through the lens of the Risk Mitigation Trade Space Framework.¹⁶ The framework contains the following elements:

- **Operational Efficiency** – What is the effect of a new security technology or procedure on operational footprint, wait times, and TSA’s workforce staffing?
- **Security Effectiveness** – What is the effect of a new security technology or procedure on TSA’s ability to detect, deter, or otherwise mitigate threats? How may adversaries shift their tactics in response to such changes?
- **Traveler Satisfaction** – What does the new technology or procedure do to improve the traveler experience?
- **Industry Vitality** – What, if any, is the economic impact of implementation? Is there an industrial base capable of supporting implementation or production of new systems?
- **Fiscal/Policy Issues** – What are the relevant issues at play and how will TSA address them?



Figure 4 TSA's Risk Mitigation Trade Space Framework

Biometrics could potentially improve the traveler experience and open the door to innovative models of public-private cooperation between TSA and aviation industry stakeholders. That said, biometric solutions raise unique issues about privacy and accuracy that are addressed later in this report.

Operational Impacts – From an operational perspective, the introduction of biometrics to the TSA checkpoint will most directly affect the TDC position. This position is staffed by a TSO who gathers boarding passes and identity credentials from each traveler in the queue to quickly perform a series of screening steps (see *Figure 5*).

The planned use of CAT will help automate *steps 1, 3, and 5*. The automation of these tasks will increase TSA’s confidence in the validity of credentials used to travel and the accuracy of the biographic data used to conduct Secure Flight vetting. CAT will also mitigate the threat of altered and counterfeit IDs, reduce the need for boarding passes at the checkpoint for many travelers (eliminate *step 4*), and automatically look up a traveler’s vetting status in near-real time from Secure Flight’s vetting engine.

The use of biometrics (for example, facial comparison) will also largely automate *step 2* by increasing assurance of identity beyond what is currently possible in a manual, human-based

¹⁶ Strategic Five-Year Technology Investment Plan for Aviation Security: 2015 Report to Congress.

operation.¹⁷ Specifically, biometrics will help mitigate threats posed by impostors using valid credentials for fraudulent purposes at the checkpoint (see subsection on *security impacts* for more detail).

For *step 6*, further integration of access control solutions with credential authentication and biometric technologies will help more fully automate the TDC process.

The development of this biometrically enabled solution will allow TSA to better secure access to the airport sterile environment and evaluate how to potentially reinvest valuable officer resources to other screening tasks. The automation of TDC functions will create a need for a ‘TSO resolution’ *step 7* in the event of system issues (for example, biometric match error, and alarm resolution).¹⁸ In the future, TSOs will oversee biometric operations at the TDC to help travelers use the technology and address issues as they happen. TSOs will continue to provide important security safeguards, including directing travelers to the correct screening lane based on the travelers vetting status.

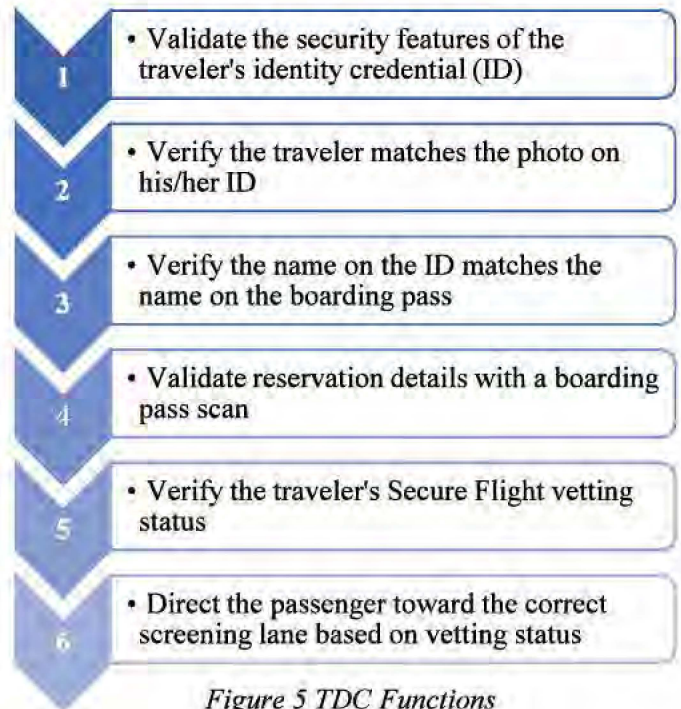


Figure 5 TDC Functions

Given the diversity of airports across the United States and their unique layouts, the operational placement and use of a fully integrated biometric solution will vary from facility to facility. For example, the use of an automated, biometric solution at a relatively small checkpoint may result in faster TDC processing times. However, the throughput of the checkpoint may be largely unaffected because a faster TDC process would merely shift traveler volume from the queue into the screening lane itself. A screening lane can only operate as fast as its slowest piece of transportation security equipment. This result underscores the need for continued investment across the entire checkpoint security enterprise.

On the other hand, at larger checkpoints with more lanes the operational efficiencies of an automated, biometric TDC may be greater. This would especially be true if the ratio of biometrically enabled TDCs to screening lanes was higher than the ratio of manual or CAT TDCs to screening lanes, thus freeing up TSO resources that could be used elsewhere. TSA will continue to explore this area as it tests checkpoint biometric solutions.

¹⁷ Except for a relatively small number of “super-recognizers,” human beings are generally outperformed by facial comparison technologies, especially when presented with the faces of persons not familiar to them such as the thousands of travelers a TSO greets and processes each day. See: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0150036>

¹⁸ Per initial modeling conducted by the Homeland Security Systems Engineering & Development Institute (HSEDI), keeping match error rates low through the use of reliable and accurate biometric systems and ensuring the use of swift error resolution procedures will be key to maintaining and improving checkpoint throughput.

In summary, the operational efficiencies TSA could gain from integrated biometric solutions may be different depending on airport facility layouts, sizes, checkpoint lane counts, and traveler volumes. New procedures and robust workforce training will be required to maximize the operational benefits of biometric solutions.

Security Impacts – TSA uses a multi-layered, risk-based approach to securing the Nation’s transportation systems. Today, during the airline reservation process, the traveler provides their first name, last name, date of birth, gender, and, if applicable, known traveler number, or DHS redress number. The airline transmits this information to TSA’s Secure Flight system for vetting against intelligence-driven watch lists. The result of this vetting process, known as the Boarding Pass Print Result, is sent to the airline and encoded on the traveler’s printed or mobile boarding pass.

When the traveler arrives at the checkpoint, the TSO must quickly perform a series of complex tasks (see *Figure 6*) using a variety of tools. TSOs assess whether the presented ID credential is authentic, determine whether the traveler matches the picture on their ID credential, decide whether the name on the boarding pass matches the name on their ID credential, distinguish between various forms of ID (state driver’s licenses, passports, and government IDs, among others), validate the boarding pass, and direct the traveler to the appropriate level of screening based on their Boarding Pass Print Result.

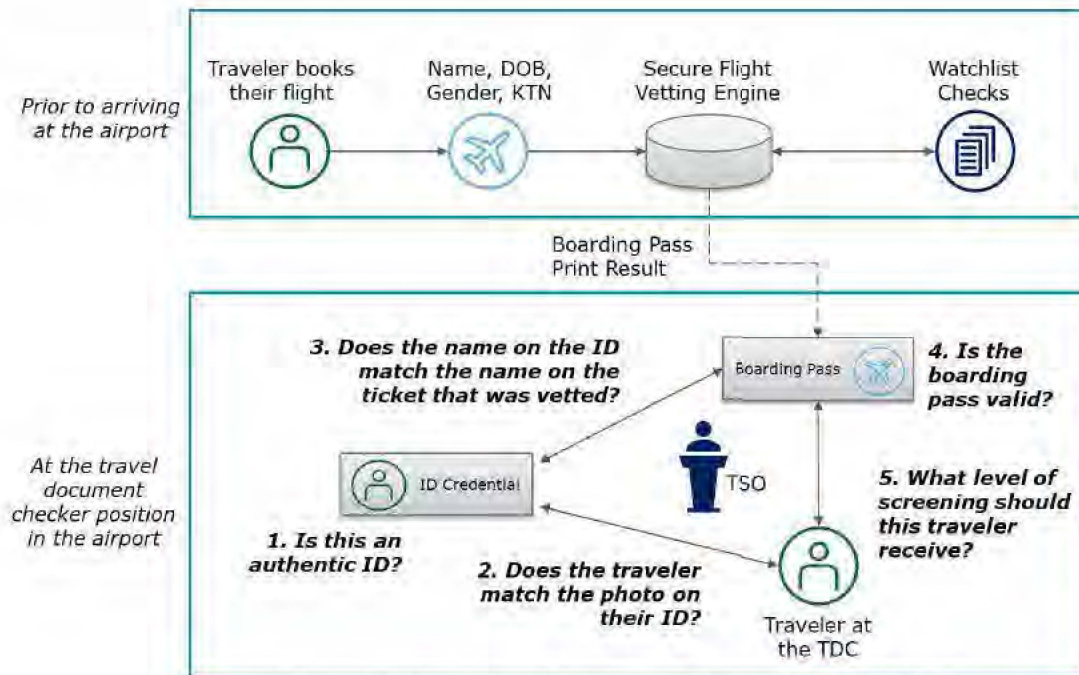


Figure 6 Systems and Operational View of Current TDC

Using an integrated, biometric TDC solution (see *Figure 7*), TSA can automate certain repetitive tasks and enable the system to verify the traveler’s identity using the facial image and biographic information encoded on the ID or through the use of previously enrolled biometric and biographic data (for example, Trusted Traveler information). This technology will help

eliminate human errors and biases in face matching, lower TSA's reliance on the boarding pass, and enable a near-real time connection to TSA vetting systems for up-to-date results.

This model shifts the burden of the security decision onto the system while reducing TSO burden of repetitive, manual face comparisons and name matching between travel documents. Automating this process will enable TSOs to focus on the operation of the systems and intervene as needed to resolve problems or process travelers who cannot or do not wish to use the biometric system.¹⁹

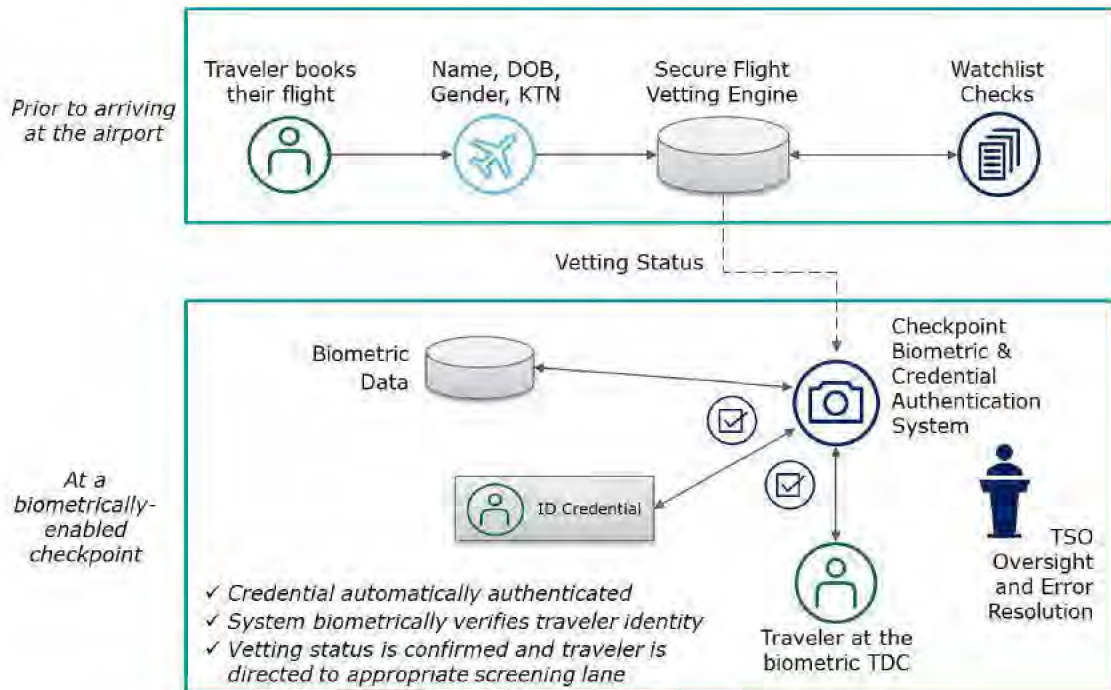


Figure 7 Systems and Operational View of Biometric TDC

Applying a biometric TDC to TSA Pre✓[®] and standard lanes would measurably increase security effectiveness and deter adversaries, or force a shift in their tactics. For example, individuals hoping to avoid detection using a fake ID or impostors using an authentic, stolen ID would be prevented from gaining access to the sterile area of the airport. In addition, integrated biometric solutions will help ensure individuals receive the correct level of screening based on their vetting status; making it more difficult for adversaries to avoid higher levels of screening by falsifying their identity.

While the rate of adversaries attempting to gain access to the checkpoint is difficult to determine, TSA can look to intelligence estimates and the experience of other organizations that use similar biometric solutions. CBP, for example, has used biometric facial comparison technology to identify more than 130 impostors trying to gain entry through air and pedestrian environments. Integrating biometrics into the checkpoint will enable TSA to further strengthen its security

¹⁹ For example, minors under age 16 without state-issued driver's licenses would still be processed using traditional boarding pass scans. Travelers who opt out to a biometric experience will also require TSO assistance to proceed into the screening lane.

~~For Official Use Only (FOUO)~~

baseline, more effectively deter and detect bad actors, and better measure performance of security measures against adversaries trying to gain access to the airport sterile environment.

IV. Potential Effects on Privacy and Mitigation Methods

As they evaluate biometric technologies, CBP and TSA are committed to protecting travelers' information and privacy. In accordance with Office of Management and Budget (OMB) Directives 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*,²⁰ any use of personally identifiable information (PII), including use of facial comparison technology, requires a thorough analysis of its privacy impact through a Privacy Impact Assessment (PIA). Both CBP and TSA have submitted and published a number of PIAs on related pilots and programs to the DHS Privacy Office for adjudication and publication. DHS PIAs use the Fair Information Practice Principles (FIPPs) to assess and mitigate any impact on an individual's privacy. These principles are rooted in the *Privacy Act of 1974* and govern the use of PII.²¹ The FIPPs help guide CBP and TSA as they seek to protect privacy and improve the traveler experience while gaining the operational and security benefits of biometrics technology.

TSA and CBP collaborate regularly with their respective Privacy Offices and DHS's Privacy Office. On September 11, 2017, the DHS Privacy Office commissioned the DHS Data Privacy and Integrity Advisory Committee (DPIAC) to advise the Department on best practices for the use of facial comparison technology. CBP briefed the DPIAC in September 2017, May 2018, and July 2018, when CBP provided a tour of biometric entry and exit operations at Orlando International Airport, and again in December 2018. The DPIAC published its report 2019-01 of the *DHS DPIAC: Privacy Recommendations in Connection with the Use of Facial Recognition Technology*,²² on February 26, 2019. CBP has implemented, and is working to implement many of the DPIAC recommendations. CBP also met with privacy and civil liberties advocates twice since 2017 to discuss the biometric entry-exit program, including technical demonstrations, the future biometric vision, privacy and security protections, notice to the public, retention policies, and alternative screening procedures. Each meeting included a lengthy question and answer session. Similarly, in August 2019, TSA held a privacy roundtable with privacy and civil liberties groups to discuss its exploration of biometrics technology.

It also noted that "it is critical for the success of the Biometric Exit Program and/or other biometric programs that data intended to be used only for screening purposes is not further transferred, shared, or used for other purposes, including without limitation private-sector purposes (e.g. marketing) or other government purposes (e.g. law enforcement or intelligence purposes)." The DPIAC's detailed recommendations will be particularly helpful as TSA and CBP consider the privacy impacts of biometrics technology.²³ For instance, TSA and CBP consider issues such as timely and transparent notice; alternative screening processes; data

²⁰ https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf

²¹ https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf; see: DHS Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, available at: <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles>.

²² [https://www.dhs.gov/sites/default/files/publications/Report%202019-01 Use%20of%20Facial%20Recognition%20Technology 02%2026%202019.pdf](https://www.dhs.gov/sites/default/files/publications/Report%202019-01%20Use%20of%20Facial%20Recognition%20Technology%2002%2026%202019.pdf)

²³ <https://www.dhs.gov/publication/dpiac-recommendations-report-2019-01>

minimization; reliability testing; data quality and integrity; accuracy; and accountability and auditability of facial comparison technology. Both agencies will address the FIPPs in their biometric technology efforts and associated privacy compliance documentation, to ensure the protection of personal information at all stages of the information lifecycle.

A. CBP Approach to Mitigating Privacy Impacts

CBP is fully committed to protecting privacy and ensuring the integrity of its facial comparison matching service. In developing and expanding the use of the TVS, CBP is implementing a privacy by design²⁴ approach to ensure that privacy protections are embedded into its use of facial comparison technology. CBP employs four primary safeguards to secure the data, including secure storage, brief retention periods, irreversible biometric templates, and strong encryption during data storage and transfer.

CBP complies with the requirements of the *Privacy Act of 1974*, as amended, the *E-Government Act of 2002*, and Departmental and government-wide policies governing the collection, use, and maintenance of PII. As with other biometric collections, facial comparison poses privacy risks that are mostly mitigated. CBP's phased deployment has illustrated the success of the use of facial comparison technology in a variety of operational scenarios, meeting CBP's business requirements while requiring minimal infrastructure investments and space redesign as well as minimal impacts upon travelers. Additionally, the approach has allowed CBP to ensure that biometrics are collected, maintained, and used consistent with privacy law and best practices. CBP analyzes the privacy impact of its collection, use, dissemination, storage, and sharing of PII through the lens of the DHS FIPPs as described above.²⁵ The eight FIPPs principles, rooted in the tenets of the *Privacy Act*, have served as the framework for privacy policy at DHS for more than a decade.

When a traveler presents himself or herself for entry, exit, or at a TSA security checkpoint, the traveler will encounter a camera connected to the biometric cloud matching service via a secure, encrypted connection. The biometric matching service converts the live photos into secure templates and matches them against templates of gallery images, which travelers have already provided to the U.S. Government for travel purposes. The templates cannot be reverse engineered to reconstruct the photo. Finally, CBP does not share any photos with travel stakeholders, but rather provides the travelers and partner airlines with the results of the biometric match (match or no-match) through a response message data value. In implementing biometric matching through the TVS, CBP is simply replacing the existing document checks with a biometric facial comparison process, which will greatly reduce the need for travelers to continually present identity documentation at multiple stops along their journey.

²⁴ See DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), available at www.dhs.gov/privacy.

²⁵ Additionally, the DHS Privacy Office conducted a Privacy Compliance Review of CBP's Southwest Border Pedestrian Exit Field Test that resulted in 10 recommendations to improve the privacy of individuals' biometric information, including facial and iris images. Available at: <https://www.dhs.gov/sites/default/files/publications/SW%20Border%20PCR%20report%20FINAL%2020161230.pdf>.

CBP provides transparency and general notification to the public through program information, such as frequently asked questions, available on the CBP website at www.cbp.gov/biometrics, and the TVS Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) published at www.dhs.gov/privacy.²⁶ The PIAs and SORNs for the TVS and its predecessor projects explain all aspects of CBP's biometric entry-exit programs, including policies and procedures for the collection, storage, analysis, use, dissemination, retention, and deletion of data. These PIAs and SORNs describe in detail CBP's approach to ensuring both the processes and systems integrate controls to mitigate privacy risks.

Following the DHS FIPP of transparency, CBP works closely with airline, airport, and cruise line partners to incorporate notifications and processes into their current business models, such as gate announcements or visible signage that explain the facial matching process and alternative inspection procedures. If processes or procedures change, CBP will update these channels to ensure all outreach material is current and clear for the traveling public. Because facial comparison can be performed quickly with minimal instruction and with a high degree of accuracy, the approach implemented represents the best operational means of verifying the identity of the traveler, and the data is collected in a manner perceived as less invasive to the traveler. Facial comparison requires no actual physical contact to collect the biometric data, and there is less risk of the loss of traveler documents that contain the date of birth and other sensitive PII.

Prior to admission into the United States, CBP must ensure that each traveler is a U.S. citizen, lawful permanent resident, or is otherwise an alien eligible for admission, and that the traveler is not attempting to import any merchandise in violation of U.S. laws. Similarly, CBP officers may inspect travelers departing the United States in order to create exit records and as required for law enforcement operations. The website www.cbp.gov/biometrics, along with signage, verbal announcements, tear sheets, and the TVS PIA contain details on the current biometric entry-exit process, including alternative procedures. In accordance with the FIPP of individual participation, a U.S. citizen and otherwise exempt aliens²⁷ may notify either the CBP officer or the airline boarding agent that he or she would like to opt out at the time of boarding and, instead, present credentials for a manual identity verification using their travel document. In adherence to the FIPP of purpose specification, CBP stipulates that PII collected through the biometric entry-exit program be used primarily to verify that the traveler attempting to board the flight or cross the border is, in fact, the rightful bearer of the travel document he or she is presenting.

Throughout its history, CBP has maintained productive partnerships with the travel industry, where the flow of PII between entities is well-defined in law and regulations. In line with the FIPPs, data minimization and use limitation, CBP has taken noteworthy steps to protect privacy,

²⁶ See DHS/CBP/PIA-056 Traveler Verification Service (November 14, 2018), available at www.dhs.gov/privacy. www.dhs.gov/privacy. The SORNs associated with CBP's Traveler Verification Service are: DHS/CBP-007 Border Crossing Information, DHS/CBP-021 Arrival and Departure Information System, DHS/CBP-006 Automated Targeting System, DHS/CBP-011 U.S. Customs and Border Protection TECS.

²⁷ Certain aliens are exempt from any requirement to provide biometrics upon entry into the United States pursuant to 8 CFR 235.1(f)(ii), or upon exit from the United States pursuant to 8 CFR 215.8.

such as its commitment to prohibit the sharing the photos captured and matched through the TVS with CBP industry partners. Only the results of the “match/no-match” determination are shared. In fact, CBP’s business requirements for partner airline and technology vendors do not permit the retention of photos for commercial purposes, following transmittal to CBP for matching. In addition, TVS only utilizes the irreversible biometric templates of source and newly-captured photos for matching and uses a unique identifier²⁸ to disassociate the biographic information associated with the new facial images.

While CBP does not retain U.S. citizens’ images submitted as part of the traveler verification process,²⁹ photos of foreign nationals (and those dual national U.S. citizens traveling on foreign documentation) are retained for up to 14 days in secure systems to confirm traveler’s identities, evaluate the technologies, and to assure continued accuracy of the algorithms. In addition, CBP transmits facial images for in-scope travelers to the DHS Automated Biometric Identification System (IDENT) for retention as the traveler’s biometric encounter with CBP. For U.S. citizens, only a confirmation of the border crossing and the associated biographic information is retained.

In line with the FIPP of accountability and auditing, the CBP Privacy Office will conduct a CBP Privacy Evaluation by the end of calendar year 2019 to ensure that all parties, including airlines, airport authorities, and cloud providers, are in compliance with the privacy protections described in the TVS PIA. The results of the evaluation will be shared with the DHS Privacy Office.

B. TSA Approach to Mitigating Privacy Impacts

TSA is committed to protecting traveler privacy and ensuring the traveling public’s trust as it modernizes identity verification through its exploration of biometric technology. TSA will comply with DHS privacy policy throughout each phase of TSA’s biometric solution development – from initial design to implementation. Solutions will be designed to secure data as it is collected, stored, and transmitted between systems to protect both travelers and system integrity.

TSA recognizes that biometric technologies, particularly facial comparison, pose unique privacy concerns with respect to privacy and passengers’ civil rights and civil liberties. There is significant risk to individuals should the facial images be compromised or used for purposes beyond those specified for its collection. There is also a risk to both individuals and transportation security in the event that the biometric technology is not sufficiently accurate. To mitigate these risks, TSA will evaluate issues such as:

- Robust notice of facial comparison deployment for traveler screening;
- Meaningful choice of screening choices for the traveler;
- Robust cyber-security measures to protect traveler data from collection through transmission to receipt; and

²⁸ The unique identifier is generated by either the travel agent, travel website hosting service, or the airline at the time of the reservation. It is comprised of a sequential number (which is only valid for the particular airline and the specific flight), plus the record locator, a six-digit code used to access additional information about the traveler.

²⁹ Photos of U.S. citizens are held in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage.

- Limitation on the use of the facial images to those necessary for transportation security, consistent with the Privacy Act.

TSA will integrate privacy protections as it continues to partner with CBP on biometrics for international travelers, implement new biometric capabilities for TSA Pre✓® travelers, and explore the expansion of biometric collections, such as use of facial images, to additional domestic travelers. TSA will also adhere to DHS privacy policy in its adoption of new biometric-based vetting solutions for non-traveler groups such as aviation workers, law enforcement officers, and crew members.

Privacy and Facial Comparison for International Travelers

Since beginning to explore the use of facial comparison technology for traveler identity verification, TSA has taken steps to provide notice to the public about its efforts, assess privacy risks, and establish strategies to protect traveler privacy. The challenge of traveler identity verification through facial comparison for TSA is significant for international and domestic travelers for whom established, government-owned facial image databases do not exist. In comparison of this challenge, TSA engaged in several pilots involving international travelers. For instance, in January 2018, a PIA was published for a three-week proof of concept at LAX using passports.³⁰ The proof of concept was to validate the use of facial comparison technology to automate identity verification during the TDC process.

TSA compared the facial images of aviation passengers with e-Passports on outward-bound international flights and who voluntarily entered the screening checkpoint through automated electronic security gates or “e-Gate.” The e-Gate device captured an image of the passenger’s face and compared it to the biometric image in the passenger’s e-Passport. The e-Gate attempted to replicate the function of the TDC and authenticated the passenger’s e-Passport and boarding pass.

Additionally, privacy protections have been embedded in TSA’s partnership with CBP on facial recognition pilots. These pilots took place in international terminals at a select number of airports to limit biometric collection to travelers on international flights. They enabled both agencies to collect data, refine solutions, and exchange information on the operational performance of facial comparison technology. Privacy compliance documents for each of these pilots have analyzed the potential effects on privacy and identified methods to lessen privacy risks.

In the first phase of the partnership, which took place in October 2017, TSA and CBP conducted an operational pilot at JFK to test the ability of CBP’s TVS to match traveler identities against galleries of pre-staged photos at the TSA checkpoint. The second phase consisted of a pilot at LAX, which tested the TVS with a larger gallery and enhanced automation, from August to October 2018. Additionally, in November 2018, TSA, CBP, and Delta Air Lines began testing

³⁰ <https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-046-tdcautomationusingfacialrecognition-january2018.pdf>

biometrics for identity verification at Terminal F at ATL. CBP published PIAs on each phase of the TVS pilot.³¹

Privacy and Biometric Solutions for TSA Pre✓® Travelers and Additional Populations

TSA is using biometrics to modernize the trusted traveler experience for TSA Pre✓® travelers. For first-time enrollees or for individuals renewing their membership in that program in person, TSA started capturing facial images to help verify identity. At this time, a facial image is not required for individuals who renew their TSA Pre✓® Application Program membership online.

TSA will also evaluate the possibility of allowing additional trusted travelers to access the TSA Pre✓® lanes (for example, members of the Department of Defense), as well as the general flying public to opt in to biometric screening and verification. However, before making biometric solutions available to these travelers, TSA will work with OBIM and DHS oversight offices, including the DHS Privacy Office and the Office of Civil Rights and Civil Liberties to evaluate options, conduct pilots, and to ensure compliance with privacy law and policy and civil rights and civil liberties requirements.

In any biometric technology solutions involving the collection, maintenance, use, or dissemination of PII, TSA will be transparent by notifying the public and explaining the steps the agency is taking to safeguard individuals' information. In its development of biometric technologies for additional populations, TSA will comply with Section 208 of the *E-Government Act of 2002*, Section 222 of the *Homeland Security Act of 2002*, and DHS' privacy compliance process. As such, TSA will conduct appropriate privacy threshold analyses, PIAs, and system of records notices when considering the use of biometric solutions with potential privacy impacts. TSA will also comply with applicable TSA, DHS, and Office of Management and Budget policies and authorities governing the handling of PII.

TSA will comply with law and DHS privacy policy related to the use of facial comparison technology for identity verification such as notice to travelers, opt-in policies, consent protocols, specific use limitations, and alternative screening procedures for travelers that do not wish to provide their facial image for identity verification purposes. Consistent with information technology security policies and authorities, TSA will also develop biometric solutions that meet cybersecurity protocols so that data is protected at all stages of the information lifecycle. Additionally, public education and outreach will be conducted to provide awareness of the agency's future biometrics efforts.

Stakeholder Engagement on Privacy

As part of its commitment to protecting traveler privacy in the use of biometrics technology, TSA will continue to:

- Engage with non-governmental stakeholders to obtain input on best practices for protecting privacy;

³¹ https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf

~~For Official Use Only (FOUO)~~

- Coordinate with internal TSA offices, DHS Headquarters, oversight entities and interagency partners to track compliance with privacy authorities and requirements, develop privacy-protective policies, and appropriately manage identified privacy risks;
- Seek information and feedback from industry, privacy groups, academic institutions, and other privacy professionals and research organizations as it considers the expansion of biometrics solutions to increase security and streamline the passenger experience; and
- Share information with key stakeholders on its development of biometrics technology capabilities.

V. TSA Methods to Analyze and Address Matching Performance Errors

While TSA has been using fingerprints since 2004 to conduct security threat assessments—including checks on an applicant’s criminal history, potential ties to terrorism, and citizenship—the use of biometrics to verify traveler identity has begun only recently. As of September 2018, the TSA Pre✓[®] Application Program has transitioned from single factor enrollment (fingerprints) to multi-modal biometric (fingerprints and facial image) enrollment. See Section II.C for an overview of TSA’s biometric testing efforts to date.

TSA’s exploration of the use of biometric data, namely facial images, as a means of facilitating secure travel is coming at an ideal time in the biometric industry. According to the most recent National Institute of Standards and Technology (NIST) Face Comparison Vendor Test, facial verification algorithms have become significantly more accurate over the 2013-2018 period. The NIST Interagency Report 8238 states:

While the industry gains are broad—at least 28 developers’ algorithms now outperform the most accurate algorithm from late 2013—there remains a wide range of capabilities. With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2 percent. The remaining errors are in large part attributable to long-run ageing and injury.³²

According to NIST, these gains have been largely facilitated by a revolution in algorithm development, fueled by new machine learning approaches. Whereas algorithms of five years ago may have struggled to match images that differed in pose, illumination, and facial expression, today’s algorithms are increasingly tolerant of such variations in image quality. Indeed, improvements to the technology are being made in months rather than years.

Despite these gains, however, facial comparison systems are shadowed by reports of variable performance across demographic characteristics; namely race, age, and gender.³³ Much of the discussion has focused on the ability of various facial comparison algorithms to accurately process younger subjects, female subjects, and subjects with darker skin. Indeed, a 2019 article published by DHS S&T and informed by testing conducted in 2018 at S&T’s Maryland Test Facility (MdTF) found evidence of some variation in facial comparison performance along

³² See NIST Interagency Report 8238, available at <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>

³³ TSA does not collect data on traveler race, ethnicity, or skin color for the purposes of making security and screening decisions; however, TSA may collect such data – in accordance with standard test protocols – during operational testing to ensure systems perform accurately under operational conditions.

demographic lines.³⁴ Interestingly, however, this performance variation was not solely based on the face comparison algorithm, but resulted from an interaction between the matching algorithm and image acquisition hardware.³⁵

S&T tested 11 commercially available facial image acquisition systems using a demographically diverse population of 363 volunteer subjects.³⁶ The live images (“probes”) gathered by each system were matched against historical and same-day enrollment images using a leading commercial algorithm for facial comparison. The variation in facial matching performance across different image acquisition systems versus when images are matched against a single, industry-leading algorithm suggests the hardware used to capture the probe image significantly affects matching accuracy.

As a result, using a superior biometric acquisition system capable of capturing higher quality facial images may significantly reduce or even eliminate performance differences along demographic lines. Logically, it follows that a lower quality acquisition system can increase the likelihood of performance variation along demographic characteristics. This key finding will influence TSA’s testing, development, and potential procurement of checkpoint facial comparison capabilities.

S&T’s recent round of testing, which took place in May and June of 2019, examined the performance of an additional 10 commercial facial acquisition systems against eight commercial facial comparison algorithms. When completed, the findings of this research may give more insight into the best mix of hardware and software assets needed to ensure the accuracy of checkpoint biometric systems for the diverse traveling public. Additionally, TSA will join interagency efforts to ensure DHS biometric systems (for example, CBP TVS, OBIM IDENT/HART) are designed to enhance performance across missions, use cases, and demographics.

Other variables encountered in the airport environment can affect system performance as well. Inconsistent lighting (for example, sun glare through large windows), changes in a traveler’s facial structure relative to previous encounter images, and eyewear or other face/head wear can affect system performance. This underscores the need for TSA to continue to invest time and energy into ensuring its checkpoint biometric solutions, as well as other transportation security equipment, are designed with the human-system interface in mind. Intuitive, highly usable solutions combined with the right TSO procedures, biometric acquisition hardware, and matching software will help ensure TSA’s mission requirements are met while also ensuring a streamlined security experience for air travelers.

³⁴ Note: S&T found “relative skin reflectance” to be a better indicator of system performance than U.S. Census categories (e.g. “White”, “Black”, and “Other”).

³⁵ See Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems, available at <https://ieeexplore.ieee.org/document/8636231>

³⁶ For more information on the S&T test facility, protocols, and results see <https://mdtf.org/rally/>.

Given the wide diversity of the millions of travelers moving through airport checkpoints daily, accuracy in biometric solutions is a key issue. Therefore, TSA is grounding its exploration of biometric solutions in rigorous scientific study and analysis to ensure the full benefits of biometrics technology are realized. Efforts will continue to ensure biometric checkpoint solutions are designed to mitigate performance variations based on demographic characteristics.

VI. Performance Assessments and Audits of the Biometric Entry-Exit Program

CBP has a robust process for performing operational assessments of CBP's biometric system performance, including evaluating the performance of biometric transactions performed during arrival and departure operations in the air environment, as well as continual performance assessments of technical demonstrations to determine the best concept of operations in other operational environments such as land and sea. Third parties such as S&T and NIST are also engaged to both evaluate CBP operational data and make recommendations for performance enhancements that include biometric capture and matching.

A. Performance Assessments

Biometric Performance Analysis of CBP Systems

CBP has a rigorous process in place to review data and metrics associated with biometric exit facial comparison matching performance. Biometric Air Exit Key Performance Parameters (KPPs) mandate that the system's True Acceptance Rate (TAR)³⁷ must equal or exceed 97 percent of all in-scope travelers and that the system's False Acceptance Rate (FAR)³⁸ must not exceed 0.1 percent of all in-scope travelers.

To establish whether or not TVS is fulfilling these KPPs, CBP is systematically analyzing actual flight data for the airlines using Biometric Air Exit. The evaluation team periodically prepares summary reports that present the actual performance of TVS against its KPPs in production.

On a weekly basis, operational performance analysis of CBP biometric operations are conducted, including Air Entry, Air Exit, Preclearance, and Pedestrian Entry (currently in technical demonstration). CBP's performance analysis is focused on the ability to match travelers captured by airports and airlines against the gallery created using the Advanced Passenger Information System (APIS) manifest. Beginning in November 2018, CBP moved to a sampling method to assess the technical match rate for biometric exit and aspects of the CBP-TSA pilot. The technical match rate is a measure of how well the matching algorithm is performing. It includes U.S. citizens who choose not to opt out and individuals who are in-scope (pursuant to 8 CFR 215 and 235) that had a photo in the CBP gallery from existing DHS sources and were

³⁷ The **TAR** is the number of valid matches divided by the sum of the valid matches and the invalid non-matches. Note that this sum (valid matches plus invalid non-matches) equals the number of matches that should have occurred, and includes all the travelers with a valid encounter photo and at least one valid gallery photo. This definition of the TAR is generally equivalent to the Technical Match Rate (TMR), as defined by CBP's Office of Field Operations.

³⁸ The **FAR** is the number of invalid matches divided by the sum of the invalid matches and the valid non-matches. Note that this sum (invalid matches plus valid non-matches) equals the number of matches that should NOT have occurred, and includes all the travelers with a valid encounter photo for whom there is no valid gallery photo.

successfully captured by the camera. The following table shows recent match results for each production mode of operation, as a per day average³⁹.

Modality	Number of Locations	Flight Count	Number of Travelers	Technical Match Rate
Air Entry	11	446	34,716	99.2%
Air Exit	16	92	11,545	97.6%
Air Preclearance	4	45	6,559	99.4%
Pedestrian Entry	4		12,591	97.7%

The estimated false positive rate based on the internal CBP analysis is .0103 percent, which is within the established KPP target of less than .1 percent. As a comparison, a 2014 study “*Passport Officers’ Errors in Face Matching*”⁴⁰, found that even individuals with specialist experience and training in the task, passport-issuing officers had a 14 percent false positive rate when conducting a person-to-photo comparison test.

Ensuring Biometric Technologies Do Not Unduly Burden Travelers

CBP continuously monitors the biometric matching service and conducts a variety of statistical tests to bolster performance thresholds and minimize any possible bias impact on travelers of certain race, gender, or nationality.

CBP requires that all airlines submit traveler information to the Advanced Passenger Information System (APIS). Among the data submitted is gender, date of birth, travel document type, number, and nationality. Using a subset of this data, CBP conducted extensive statistical analysis including *chi squared*⁴¹ independence tests to determine whether traveler demographics (age, gender, and nationality) affect facial comparison match rates. As CBP does not collect race/ethnicity nor is this information included in the APIS manifest, citizenship is used as a proxy to conduct its analysis.

CBP’s analysis found a negligible effect in regards to biometric matching based on citizenship⁴², age, or gender while achieving a technical match rate (TMR) in the high 90 percentile.⁴³ As of December 2018, TMR continues to be at a steady state, above 98 percent. Significant improvements to the algorithm and exit operations continue to be made, which has led to a substantial reduction in the initial gaps in matching for ages and genders. On average, U.S.

³⁹ Data shown indicates the averages per day for the period March 20, 2019 to April 2, 2019.

⁴⁰ <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0103510>

⁴¹ A *chi-squared* (χ^2) independence test is a statistical test applied to sets of categorical data to evaluate how likely it is that any observed difference between the sets arose by chance. The tests can be used to determine whether there is a significant difference between the expected frequencies and the observed frequencies in one or more categories.

⁴² While CBP uses citizenship as a general proxy because it does not collect race/ethnicity data, it takes into account in its analysis that this is clearly a more effective proxy when looking at homogenous countries than diverse ones.

⁴³ Based on June 2017 – November 2018 CBP Air Exit data from biometric exit locations: JFK, MIA, IAH, HOU, ORD, SEA, SFO, LAS, DTW, LAX, IAD, MCO, ATL, BOS, and FLL.

citizens typically match at a lower rate as they have fewer and older photos which decreases matching rates. Travelers between ages 26 and 65 match slightly better than “young” (ages 14 to 25) travelers (0.3 percent) and “old” (ages 66 to 79) travelers (0.1 percent), compared to 2.8 percent and 8 percent, respectively, during the initial pilot period. Similarly, women match slightly better than men (0.2 percent), compared to matching worse initially (1.7 percent) during the pilot period. Much of the bias seen in the initial period also relates to much lower flight volume during that timeframe.

As NIST concluded during its 2018 Face Comparison Vendor Test⁴⁴, there have been massive improvements in the accuracy of face comparison algorithms in the last five years (2013-2018). The performance of CBP’s TVS continues to improve over time due to technical, operational, and procedural advancements including threshold adjustments and testing multiple vendors. CBP has enhanced the photo selection process used to build the galleries, which reduces the number of travelers with no photos and improves the accuracy of the system.⁴⁵ Additionally, CBP has enhanced the manner in which the galleries are populated, ensuring that the information included in the flight manifest is used to its maximum potential to include more higher-quality photographs.⁴⁶ CBP has also issued various update to the matching algorithms, which increase the algorithm’s ability to create biometric templates from non-frontal images taken during the U.S. entry or exit process.

There have also been software changes to the cameras to allow travelers posing for the photos to receive visual feedback. Furthermore, as CBP continues and expands its usage of TVS, personnel using the technology become more aware of the optimal camera positions to ensure better images and increase the traveler throughput. Some cameras are also now equipped with multiple lenses to capture images for various angles, which may increase photo quality depending on the height of the traveler.

Biometric Technology Impact on Travelers Overstaying Their Lawful Period of Admission

CBP has the ability to accurately report overstay numbers in the air and sea environments today. In FY2018, DHS calculated a total overstay rate of 1.22 percent, or 666,582, overstay events. In other words, 98.78 percent of in-scope nonimmigrant entries in FY2018 departed the United States on time and in accordance with the terms of their admission. Annual statistics on visa overstays are provided by DHS to Congress in the Annual Entry Exit Overstay Report.⁴⁷

Adding biometric verification to an already robust biographic exit capability enables CBP to better detect travelers seeking to depart the country under a false identity, including aliens

⁴⁴ See NIST Interagency Report 8238, available at <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>.

⁴⁵ A 2010 NIST evaluation of face comparison showed that considerable accuracy benefits accrue with retention and use of all historical images. See <https://www.nist.gov/publications/report-evaluation-2d-still-image-face-recognition-algorithms>.

⁴⁶ Additional information about CBP’s gallery building process can be found in the DHS/CBP/PIA-056, Privacy Impact Assessment for the Traveler Verification Service, issued Nov. 14, 2018, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf.

⁴⁷ See FY 2018 Entry-Exit Overstay Report at: https://www.dhs.gov/sites/default/files/publications/19_0417_fy18-entry-and-exit-overstay-report.pdf

seeking to fraudulently use validly issued U.S. travel documents. The addition of biometrics has assisted CBP officers in detecting impostors attempting to gain entry to the United States. As part of the continued expansion of biometric exit capabilities, CBP will measure and report on the number of impostors detected by the biometric exit program.

Utilizing biometric technology, CBP has been able to biometrically confirm more than 14,000 travelers that overstayed their lawful period of admission on exit. As of April 2019, 130 impostors have been positively identified using the TVS system across air entry and pedestrian entry environments. All biometric encounters of in-scope foreign nationals are recorded in the enterprise biometrics system IDENT.

B. Audits Performed

DHS Office of Inspector General

The DHS Office of Inspector General (OIG) audit (OIG-18-80), *Review of CBP Biometric Exit Capability*⁴⁸, evaluated CBP's efforts to develop and implement a biometric exit capability and assess whether biometric data collected has improved DHS's ability to verify foreign visitor departures at U.S. airports. The final report was issued on September 24, 2018, and included four recommendations:

- 1) Develop an internal plan to institute enforcement mechanisms or back-up procedures to prevent airlines from bypassing biometric processing prior to flight boarding;
- 2) Take steps to coordinate with airport and airline stakeholders to increase bandwidth to meet the operational demands of biometric processing at the Nation's top airports;
- 3) Continue to refine the TVS algorithm to ensure the highest possible traveler match rate, with allowances for photo age and quality; and
- 4) Develop internal contingency plans for funding and staffing the program, in the event that airlines do not agree to partner with CBP in implementing the biometric capability nationwide.

The OIG conducted fieldwork from September 2017 to January 2018 and reviewed data from the earliest start of the technology demonstrations, which were never intended to be a final implementation model. However, regarding recommendation three and as addressed previously in this report, CBP continues to monitor and improve algorithm performance through incremental updates and improvements with system development and image quality requirements. CBP data analytic teams are evaluating any anomalies and providing feedback to development teams to improve entity resolution and refine matching performance

DHS Science and Technology (S&T) Directorate

In order to continually improve upon the quality of the images, DHS S&T is assisting CBP by testing the efficiency, effectiveness, user satisfaction, and equitability of biometric systems. This

⁴⁸ Available at: <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf>.

includes performing independent scenario testing of state of the art commercial biometric systems at the MdTF as well as performing analyses using a sample of operational TVS images.

Starting in 2018, DHS S&T has performed independent biometric analyses using a sample of operational TVS probe and gallery facial images⁴⁹⁵⁰. These analyses focused on answering specific questions regarding biometric performance. DHS S&T found that the algorithm used in TVS was superior in performance to all other algorithms tested.

Calculating standard biometric performance metrics in operational systems is challenging. DHS S&T developed a method for estimating the false positive identification rate (FPIR) using operational TVS system data. DHS S&T presented the new method, termed “Virtual Red Team” analysis, to CBP. DHS S&T used this method to estimate FPIR. DHS S&T concluded that FPIR for TVS varies by flight, such that some flight routes could have FPIR values 6-fold higher than others.

Based on these analyses, DHS S&T made specific recommendations to CBP including:

1. To ensure that only ticketed travelers are allowed to use TVS for boarding OR to increase match thresholds used for biometric exit; and
2. To carry out an exhaustive “Virtual Red Team” analysis to calculate the risk of false matches based on the demographics (age, country of origin, gender) of travelers on individual flights.

National Institute of Standards and Technology

CBP is also collaborating with NIST to perform an independent and comprehensive scientific analysis of CBP’s operational face matching performance, including impacts due to traveler demographics and image quality. This independent study will help verify results and provide a more in-depth analysis on various factors. Upon analyzing a comprehensive set of data, NIST will provide objective recommendations regarding matching algorithms, optimal thresholds, and gallery creation, optimizing face matching performance for large-scale traveler ID at air, land, and sea entry and exit ports of entry. CBP will continue to actively monitor and refine the performance of this process and associated algorithms in order to make incremental improvements and minimize signs of bias, and ensure the high accuracy of facial matching for all travelers.

⁴⁹ DHS S&T Port of Entry- People Screening. February, 2018. Analysis of Data and Algorithms Related to the Traveler Verification System: Estimating Effects of Gallery Size and Traveler Demographics on False Positive Identification Rates.

⁵⁰ DHS S&T Biometric and Identity Technology Center. January, 2019. Analysis of Data and Algorithms Related to the Traveler Verification System: Estimating False Match Rate and False Positive Identification Rate.

VII. Conclusion

Biometric technologies have the potential to greatly enhance operational efficiencies and security for both CBP and TSA. CBP has made significant progress in implementing biometric solutions across air, land, and sea since receiving the biometric entry-exit mission in 2013. Following publication of the joint policy memorandum on CBP and TSA's partnership on the development and implementation of biometric technologies, particularly facial comparison, both agencies have worked together on a number of operational pilots. These volunteer-based pilots have allowed both agencies to test, evaluate, and continue to refine biometric technology solutions, while working to achieve a more streamlined traveler experience. CBP and TSA's efforts have been grounded in transparency and a commitment to traveler privacy. CBP and TSA will continue to work together and seek input from their stakeholders as they examine the impact of biometric technology and work to align with DHS initiatives, strategies, and capabilities on biometrics.

VIII. Appendices

Appendix A. DHS Fair Information Practice Principles

Transparency	DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
Individual Participation	DHS should involve the individual in the process of using PII, and to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII.
Purpose Specification	DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.
Data Minimization	DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
Use Limitation	DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
Data Quality and Integrity	DHS should to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
Security	DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
Accountability and Auditing	DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Appendix B. Acronyms

Acronym	Definition
APIS	Advance Passenger Information System
ATL	Hartsfield-Jackson Atlanta International Airport
CAT	Credential Authentication Technology
CBP	U.S. Customs and Border Protection
DCA	Ronald Reagan Washington National Airport
DHS	U.S. Department of Homeland Security
DPIAC	Data Privacy and Integrity Advisory Committee
FAR	False Acceptance Rate
FIPP	Fair Information Practice Principles
FOUO	For Official Use Only
FPIR	False Positive Identification Rate
FY	Fiscal Year
HART	Homeland Advanced Recognition Technology
HSSEDI	Homeland Security Systems Engineering & Development Institute
ID	Identification
IDENT	DHS Automated Biometric Identification System
JFK	John F. Kennedy International Airport
KTN	Known Traveler Number
KPP	Key Performance Parameters
LAX	Los Angeles International Airport
MdTF	S&Ts Maryland Test Facility
NIST	National Institute of Standards and Technology
OBIM	Office of Biometric Identity Management
OIG	DHS Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	personally identifiable information
S&T	DHS Science and Technology Directorate
SORN	System of Records Notices
TAR	True Acceptance Rate
TDC	Travel Document Checker
TMR	Technical Match Rate
TSA	Transportation Security Administration
TSO	Transportation Security Officer
TVS	Traveler Verification Service

Table of Contents

Revision History iii

Executive Summary 4

Section 1: Introduction 5

1.1 Background 5

1.2 Purpose 5

1.3 Scope 9

1.4 Study Team/Organization 9

1.5 AoA Review Process 9

1.6 Schedule 9

Section 2: Conditions and Assumptions 10

2.1 Air Exit Scenarios 10

2.2 Land Scenarios 11

2.3 Sea Scenarios 12

2.4 Hazards 13

2.5 Environment 13

2.6 Assumptions 13

2.7 Constraints 13

Section 3: Determination of Effectiveness Measures 14

3.1 Mission Activities/Processes and Tasks 14

3.2 Measures of Effectiveness and Performance 14

Section 4: Alternatives 14

4.1 Description of Viable Alternative(s) 14

4.2 Non-Viable Alternatives 16

4.3 Concept of Operations (CONOPS) 17

4.4 Supportability/Sustainment Concepts 17

4.5 Interoperability Concepts 18

4.6 Market Research 18

Section 5: Methodology and Analysis Results 18

5.1 Models, Simulation and Source Data 18

5.2 Synopsis: Entry/Exit Analysis of Experiments 18

Section 6: Recommended Alternative and Rationale 26

Appendix A: Acronyms 27

Revision History

Date	Section	Description
June 1, 2017	All	Initial Version
July 18, 2017	All	Corrections to grammar, punctuation and syntax, handling of acronyms; inserted Appendix (Acronyms)
July 24, 2017	5.2	Inserted Synopsis, Entry/Exit Analysis of Experiments

Executive Summary

Since receiving the Entry/Exit mission in 2013, U.S. Customs and Border Protection (CBP) has conducted several experiments at air and land ports of entry, integrating biometrics designed to inform and refine entry and exit requirements, operational processes and shape a long-term biometric exit solution in all environments. From these trials, CBP has developed a realistic and achievable biometric exit plan.

The findings and lessons learned from these experiments are documented in Appendix A—Analysis of Experiments (AoE). The AoE provides the rationale for the decision to use the traveler’s facial image as the biometric modality to confirm identity. As such, this Analysis of Alternatives (AoA) for the Biometric Entry-Exit Program is a departure from the traditional AoA. [REDACTED] (b) (7)(E)

[REDACTED]

[REDACTED] (b) (5)

[REDACTED] (b) (7)(E)

The DIST and AEER experiments showed that a token-less face recognition scenario utilizing available CBP passenger photos could meet accuracy and throughput requirements for air (and by extension sea) exit. On-going air exit pilot projects extend the DIST results by showing that scenarios with different traveler demographics, different face capture technologies and processes and backend matching instead of local matching also meet throughput and accuracy requirements. [REDACTED] (b) (5)

[REDACTED] (b) (5)

[REDACTED] (b) (5). For vehicle land exit, preliminary results from Oak Ridge National Labs provide evidence that good quality face images can be captured from passengers in moving vehicles at exit. To meet the expedited timeframe to deploy a biometric entry-exit solution, CBP determined that engaging in further experimentation was unnecessary as the results of these experiments were deemed sufficient to validate the program’s operational scenarios and requirements.

This AoA identifies three main capability needs that CBP requires to biometrically verify all travelers as they exit the U.S. These capability needs are: Verify Traveler Identity, Create and Manage Biometric Records, and Generate Metrics and Reports. The AoA summarizes how each experiment addressed various aspects of these capability needs, operational scenarios and the resulting operational and technical requirements that continue to inform the direction that the Biometric Entry-Exit Program is following to

deliver required biometric identification capabilities. These experiments have enabled CBP to develop several Measures of Effectiveness (MOE) and Measures of Performance (MOP) that are documented in the AoA and Operational Requirements Document (ORD) and will be used to measure progress over the life of the program. The experiments helped to establish cost parameters for a nationwide solution that have been incorporated into the initial Spend Plan that was approved by DHS and the Office of Management and Budget in January 2017 and into the program's Lifecycle Cost Estimate (LCCE) that is being developed as part of the Acquisition Decision Event-2A milestone.

Section 1: Introduction

1.1 Background

In 1996, Congress passed legislation mandating the creation of a biographic entry and exit system. After the 9/11 attacks and the formation of DHS, Congress added biometrics as a requirement of the entry and exit system. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) office was created to implement a biometric entry and exit system for non-citizens entering and departing the United States. Every day CBP processes over 1 million travelers as they enter the U.S. at air, land, and sea Ports of Entry (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. To meet CBP's response time requirements, queries had to be executed on a one-to-one basis using the travel document as the search key to identify the exact prints on file. Although this had a significant and positive impact on CBP's law enforcement mission, it added time and complexity to the arrivals process and did little to provide a facilitation benefit.

While the entry system was being deployed, and utilized there was little advancement towards a biometric exit solution. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program led several field tests and experiments, but no operational capability was completed. In late 2013 Congress transferred the biometric exit mission to CBP for execution.

In 2014 DHS Science and Technology (S&T), working with CBP evaluated biometric technologies and operational processes under simulated airport entry and exit conditions. In 2015, CBP conducted additional field tests/experiments to test technologies for collecting and matching biometrics of travelers at air and land (POEs).

In fiscal year 2016, Congress authorized the Consolidated Appropriations Act (P.L. 114-113) which includes up to \$1 billion over a period of 10 years for the implementation of a biometric entry-exit program. This was followed on March 6, 2017 by Executive Order 13780: Protecting the Nation from Foreign Terrorist Entry into the United States, Sec.8, and expedited completion of the Biometric Entry-Exit Tracking System.

1.2 Purpose

The purpose of the Analysis of Alternatives is to summarize the objectives and results for each of the relevant biometric experiments. The results of the analysis for each alternative are provided and the recommended preferred alternative is identified with a detailed rationale for this recommendation.

1.2.1 Mission and Goals

The primary mission for 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 and conveyances to determine admissibility to the U.S. and enforce and administer U.S. immigration laws.

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.

Under existing laws and Executive Order 137801, 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 USCIs, 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 another authorized travel document. Biometric data includes information captured from fingerprints, facial images, or other characteristics that are unique to an individual. Biographic data, when used with biometric 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 USCIs, is now a reality for all modes of transportation.

CBP recognizes that biometric technology has multiple uses across DHS. (b) (5)
(b) (5)
(b) (5)
(b) (5)
(b) (5)
(b) (5)
(b) (5)
(b) (5)

1.2.2 Capabilities Required

The necessary capabilities needed to accomplish the biometric entry-exit mission are as follows:

1. Verify Traveler Identity
 - a. Capability Description: The ability to capture, review, analyze, search, and match all traveler's biometric information to their biometric and biographic

¹ <https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreign-terrorist-entry-into-the-united-states>

FOR OFFICIAL USE ONLY

records when entering and exiting the U.S. for the purposes of verifying their identity.

b. Capability Attribute Description

- Operational (Functional) Attributes:
 - Fast, efficient biometric data collection
 - Real-time biometric matching of collected data to stored traveler information
 - Pre-positioned traveler information to CBP Officers (CBPOs) for quick, reliable and accurate traveler assessment upon entry, or prior to exiting the country

2. Create and Manage Biometric Records

a. Capability Description: The ability to capture, store, and disseminate biometric information and metadata collected from travelers entering and, where required, exiting the U.S.

b. Capability Attribute Description

- Operational (Functional) Attributes:
 - Identity verification using biometric data collection and real-time matching of traveler information
 - Pre-positioned traveler information to CBP Officers for quick, reliable and accurate traveler assessment upon entry, or prior to exiting the country
 - Controlled exit environment to ensure traveler departure with minimal impact or delays
 - Border crossing record history on all travelers

3. Generate Metrics and Reports

a. Capability Description: The ability to measure and report the effectiveness of the biometric entry-exit system.

b. Capability Attribute Description

- Operational (Functional) Attributes:
 - Accurate, comprehensive, current data for assessing the efficiency and effectiveness of the end-to-end system
 - Readily accessible data to ensure effective monitoring of the operational environment

1.2.3 Current Situation

Today, CBP collects fingerprints and facial images from most foreign visitors entering the U.S., and uses the biometric database operated by OBIM to confirm identity.

(b) (5)

(b) (5)

(b) (5) Biometric matching capabilities are being developed by CBP OIT and its impacted components. The Traveler Verification Service (TVS), developed by OIT to support the Air Exit pilot projects, is designed as a common face recognition service that allows other CBP users to enroll images and perform face identification functions.

(b) (7)(E)

1.2.4 Gaps

(b) (7)(E)

(b) (7)(E)

1.

(b) (7)(E)

- d. [REDACTED] (b) (7)(E)
[REDACTED]
 - e. Facilities: CBP will need to ensure that facility constraints at all POEs are included in assessing solution approaches before committing to a technology solution.
 - f. Regulations: The Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law No. 104-208, Div. C, 110 Stat. 3009-546 (Sept. 30, 1996) mandated the development of a biometric exit system for all travelers leaving the U.S.
2. Capability Gap #2 Create and Manage Biometric Records
- a. Doctrine: CBP lacks a clear and approved regulation and policy addressing the collection and use of biometrics on exit.
 - b. Materiel: CBP lacks sufficient network infrastructure and storage capacity for biometric data.
 - c. Regulations: Regulatory language and completion of a rule making process may be required to implement biometric collection on exit. Case law has not been established concerning the issue of biometric collection and will remain open until resolved.
3. Capability Gap #3 Generate Metrics and Reports
- a. Materiel: CBP lacks report generating capability required to support mission objectives and system effectiveness. A robust reporting system must be designed and implemented to ensure proper support for a biometric entry-exit program.

1.3 Scope

The scope of this AoA is to describe the biometric entry-exit field tests/experiments that were conducted to determine the preferred biometric modality and feasibility of the proposed entry-exit solution across multiple operational environments.

1.4 Study Team/Organization

Experiments were coordinated by the CBP Office of Field Operations (OFO) with the CBP Office of Information and Technology (OIT) and the United States Department of Homeland Security Office of Science and Technology (DHS S&T).

1.5 AoA Review Process

[REDACTED] (b) (5)
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

1.6 Schedule

The following table depicts the actual timeframes in which each of the biometric experiments were conducted.

Biometric Field Test Name	Operational Test Start	Report Complete
Air Entry/Exit Re-engineering (AEER) Project	April 2013	October 2015
1:1 Facial Comparison Experiment	March 2014	December 2015
Biometric Exit (BE) Mobile Experiment (Fingerprints)	March 2014	June 2016
Departure Information System Test (DIST) (Face)	October 2015	December 2016
Pedestrian Field Test at Otay Mesa (Face/Iris)	December 2013	October 2016

Table 2 – Biometric Experiment Schedule

Section 2: Conditions and Assumptions

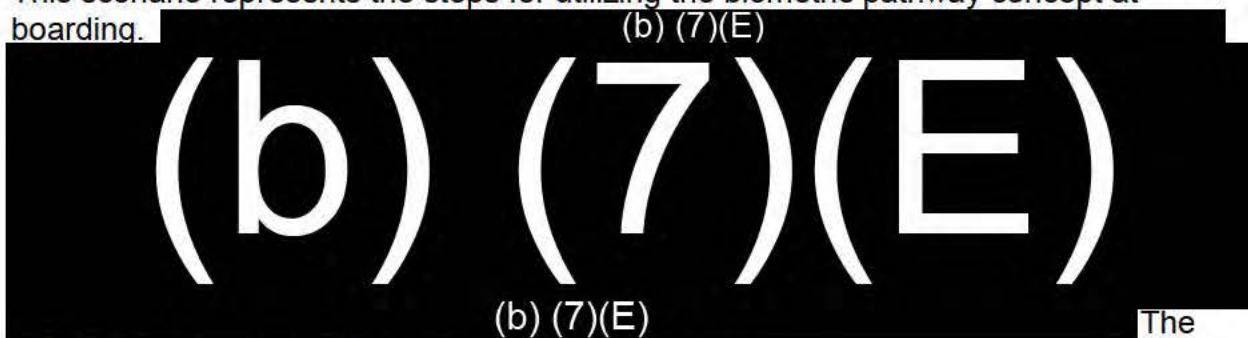
2.1 Air Exit Scenarios

2.1.1 Pre-Travel: Building Targeted, Temporary Biometric Galleries

Prior to travel, airlines will continue to submit biographic passenger manifest data from their reservation systems to CBP through APIS interfaces. The Biometric Entry-Exit Program will utilize APIS manifest data to search CBP and other government holdings for existing traveler facial images to build small, temporary, targeted biometric galleries. These galleries are then used by CBP's TVS to match live facial images submitted by stakeholders during the travel process to verify traveler identity.

2.1.2 Air Exit Boarding Scenario

This scenario represents the steps for utilizing the biometric pathway concept at boarding.



following steps identify the air exit boarding scenario:

1. Traveler approaches the boarding gate
2. Biometrics are captured
3. Biometrics are submitted to CBP
4. CBP performs matching and automated analysis
5. CBP provides response to airline with travelers' biometrically confirmed identity and authorization to proceed
6. CBP records crossing as biometrically confirmed in OBIM/ Automated Biometric Identification System (IDENT), CBP Arrival Departure Information System (ADIS) and TECS
7. Traveler boards the aircraft

2.2 Land Scenarios

(b) (5)

2.2.1 Pre-Travel

(b) (5)

2.2.2 End State Pedestrian Exit

(b) (5), (b) (7)(E)

(b) (5), (b) (7)(E)

(b) (5), (b) (7)(E)

1. (b) (5), (b) (7)(E)
2. (b) (5), (b) (7)(E)
3. (b) (5), (b) (7)(E)
4. (b) (5), (b) (7)(E)
5. (b) (5), (b) (7)(E)
6. (b) (5), (b) (7)(E)

2.2.3 End State Vehicle Exit

(b) (5), (b) (7)(E)

1. (b) (5), (b) (7)(E)
2. (b) (5), (b) (7)(E)

(b) (5), (b) (7)(E)

1. (b) (5), (b) (7)(E)
2. (b) (5), (b) (7)(E)
 - a. (b) (5), (b) (7)(E)
 - b. (b) (5), (b) (7)(E)
3. (b) (5), (b) (7)(E)
4. (b) (5), (b) (7)(E)
5. (b) (5), (b) (7)(E)
6. (b) (5), (b) (7)(E)

2.2.4 Commercial Bus Exit

(b) (5), (b) (7)(E)

2.3 Sea Scenarios

(b) (5), (b) (7)(E)

2.3.1 Pre-Travel

(b) (5), (b) (7)(E)

2.3.2 Embarkation

(b) (5)

1. (b) (5)
2. (b) (5)

- 3. [REDACTED] (b) (5), (b) (7)(E)
- 4. [REDACTED] (b) (5), (b) (7)(E)
- 5. [REDACTED] (b) (5), (b) (7)(E)
- 6. [REDACTED] (b) (5), (b) (7)(E)

2.4 Hazards

[REDACTED] (b) (7)(E)

2.5 Environment

2.5.1 Air Operating Environment

[REDACTED] (b) (5)

2.5.2 Land Operating Environment

[REDACTED] (b) (5)

2.5.3 Sea Operating Environment

[REDACTED] (b) (5)

2.6 Assumptions

- 1. [REDACTED] (b) (5), (b) (7)(E)
- 2. [REDACTED] (b) (5), (b) (7)(E)
- 3. [REDACTED] (b) (5), (b) (7)(E)
- 4. [REDACTED] (b) (5), (b) (7)(E)

2.7 Constraints

- 1. [REDACTED] (b) (7)(E)

- 2. [REDACTED] (b) (7)(E)
- 3. [REDACTED] (b) (7)(E)
- 4. [REDACTED] (b) (7)(E)

Section 3: Determination of Effectiveness Measures

3.1 Mission Activities/Processes and Tasks

Biometric entry-exit will leverage existing CBP systems and data, utilize enterprise services, existing physical facilities and infrastructure, and biometric data collected from travelers arriving and exiting the U.S. [REDACTED] (b) (5)

[REDACTED] (b) (5)

3.2 Measures of Effectiveness and Performance

[REDACTED] (b) (5)

Please see Appendix A: Biometric Entry-Exit Program Analysis of Experiments dated March 2017, p. 10-15 for a complete list of Measures of Effectiveness and Performance that were examined.

Section 4: Alternatives

4.1 Description of Viable Alternative(s)

Facial Image

CBP recognizes that facial recognition like all biometrics including iris and fingerprints have match accuracy limitations. However, accuracy is just one of several system characteristics that contribute to the viability of a particular modality for a specific operational scenario. Consideration of parameters such as availability of images, user acceptance, ease and timing of capture, processing time and associated throughput all support CBP's decision to use facial recognition. Analysis of the results from the experiments detailed below using a variety of face image capture technologies and capture procedures show that facial recognition performance in challenging operational environments with broad demographic characteristics is robust. [REDACTED] (b) (5)

(b) (5)

4.1.1 1:1 Face

During the 1:1 Facial Comparison experiment, a commercial off-the-shelf camera and devices were integrated into the air entry process to perform one-to-one verification of a live traveler photo against the traveler's passport photo in the e-passport chip. CBP was able to successfully demonstrate that facial comparison technology can assist CBPOs in verifying that the person presenting a travel document is the true owner of that document with minimal impact to travelers and overall processing time.

4.1.2 Pedestrian Exit

The Pedestrian Exit Field Test added a biometric collection component to the land entry process and changed the way in which pedestrian travelers enter and leave the U.S. via the Otay Mesa port of entry. CBP captured facial and iris biometrics from in-scope travelers and enrolled the biometrics into searchable databases for out-bound matching.

(b) (7)(E)

Overall, the experiment showed that facial capture technology was more successful than iris in unsupervised scenarios and that the operational rejection rate was much lower for face than for iris.

4.1.3 Biometric Exit – Mobile (BE-Mobile)

The objective of the BE-Mobile experiment was to investigate the feasibility of using hand-held biographic and biometric (fingerprint) capture devices to support air exit processing and law enforcement operations. The experiment resulted in a (b) (7)(E) fingerprint capture rate of which (b) (7)(E). Total processing time was (b) (7)(E) on average and no flights were delayed during the experiment.

4.1.4 Departure Information System Test (DIST)

During DIST, a pre-departure process was used to prepare a face matching gallery for passengers on a flight in the air exit environment. During departure, passenger face images were captured and matched against the gallery. Post-departure, the match performance was analyzed (albeit not in real-time). The experiment found an average scanned passenger match rate of (b) (7)(E) and an average biometric transaction time (the time between taking a photo and matching it to the gallery) of (b) (7)(E) with a total average transaction time of (b) (7)(E).

4.1.5 Air Entry Exit Re-Engineering (AEER) Laboratory Testing

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)
[Redacted]

(b) (7)(E)
[Redacted]

(b) (7)(E)
[Redacted]

(b) (7)(E)
[Redacted]

4.2 Non-Viable Alternatives

Fingerprint

Although used by many Federal agencies, the use of fingerprints to validate identity for all travelers is limited primarily by the availability of fingerprints for all traveler segments, specifically USCs. As discussed in Section 1.2.3, CBP does use fingerprint collection to verify identity of all visitors entering the U.S.; CBP does not perform the same procedure on USCs at entry. For fingerprints to be useful in biometric matching, the government would need to require the enrollment of fingerprints from all USCs so that biometric matching could be performed quickly and reliably. (b) (5)

(b) (5)
[Redacted]

Iris

The Pedestrian Exit Experiment identified that iris capture and matching in an outdoor operational environment was not feasible from an operational aspect as it was difficult for travelers to adjust their normal behavior when interacting with the iris capture device. Additionally, the iris capture devices required too much interaction from CBP personnel in helping a traveler submit to iris capture in a seamless manner for additional consideration as a biometric modality that could be used at CBP exit locations. (b) (5)

(b) (5)
[Redacted]

4.3 Concept of Operations (CONOPS)

CBP will implement a biometric matching capability to be used by third-party stakeholders in the travel industry or by CBP itself to identify travelers throughout the travel process. The capability will leverage existing government holdings to create small, targeted biometric galleries of expected travelers based upon travel manifest data.

(b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

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

The solution will ensure privacy and compliance with all applicable privacy policies, procedures and internal controls necessary to safeguard personally identifiable information (PII) pursuant to the Privacy Act.

4.4 Supportability/Sustainment Concepts

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. These factors are designed to maximize program efficiency and drive down costs. As the operational plans are developed and acquisition approaches finalized, cost savings will be assessed and will inform the Integrated Logistics Support Plan (ILSP).

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 - The functional requirements for Operations and Maintenance will ensure maximum, sustained operational availability of the biometric matching service. A two-pronged approach of regularly scheduled preventive maintenance on a quarterly basis, with immediate response for corrective maintenance, ensures that all systems and equipment will perform to the highest performance standards over their lifecycle, thereby 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 – (b) (7)(E) [Redacted]

4.5 Interoperability Concepts

CBP’s biometric matching service capability for entry-exit will interface with CBP, DHS and other government systems to build biometric galleries using existing government holdings, biographically and biometrically search watch lists, biometrically confirm crossings, and match arrival and departure records. (b) (7)(E) [Redacted]

4.6 Market Research

OIT reached out to industry experts (b)(4), (b)(7)(E) and DHS S&T) to determine alternate solutions to Biometric Exit Verification. (b) (7)(E) [Redacted]

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]
4. (b) (7)(E) [Redacted]
5. (b) (7)(E) [Redacted]
6. (b) (7)(E) [Redacted]
7. (b) (7)(E) [Redacted]

Section 5: Methodology and Analysis Results

5.1 Models, Simulation and Source Data

See Appendix A: Biometric Entry-Exit Program Analysis of Experiments dated March 2017 for detailed summary of experiment findings and operational effectiveness analysis.

5.2 Synopsis: Entry/Exit Analysis of Experiments

5.2.1 AEER Laboratory Experiments/Field Tests

(b) (7)(E)

[Redacted]

**Passive Unimpeded Boarding Gate
Objective:**

(b) (7)(E)

[Redacted]

Description/Scenario:

(b) (7)(E)

[Redacted]

Results:

(b) (7)(E)

[Redacted]

Recommendation:

(b) (5), (b) (7)(E)
[Redacted text block]

Biometric Transaction Terminal (BTT) Face Verification Objective:

(b) (7)(E)
[Redacted text block]

Description/Scenario:

(b) (7)(E)
[Redacted text block]

Results:

(b) (7)(E)
[Redacted text block]

Recommendation:

(b) (5), (b) (7)(E)
[Redacted text block]

Passive Surveillance Mode Facial Recognition on Passenger Bridge Objective:

(b) (7)(E)

Description/Scenario:

(b) (7)(E)

Results:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Recommendation:

(b) (5), (b) (7)(E)

5.2.2 Entry/Exit Transformation (EXT) Experiments

(b) (7)(E)

**1:1 Face ePassport Air Entry Experiment:
Objective:**

(b) (7)(E)

Description/Scenario:

FOR OFFICIAL USE ONLY

The Face system collects the traveler's facial image at the booth and matches it to the image stored in the traveler's ePassport chip. The images and matching results are displayed on the monitor to assist the CBPO in verifying the traveler's identify as part of the admissibility inspection process.

Results:

(b) (7)(E)

[Redacted]

(b) (7)(E)

[Redacted]

Recommendation:

(b)(5), (b)(7)(E)

[Redacted]

Pedestrian Exit Field Test:

Objective: Introduce a biometric collection component to the entry process and evaluate the way in which pedestrian travelers enter and leave the U.S. and evaluate results of the altered in-bound process.

Description/Scenario:

At inbound inspection, CBP captured a facial and iris image from in-scope travelers at kiosks and enrolled the biometrics into searchable databases to be used for out-bound

matching. Pedestrians wishing to exit the U.S. presented their documents for scanning or reading at an automated exit station deployed in lanes in the outbound area. If the traveler was determined to be of law enforcement interest, CPBOs took appropriate enforcement measures per operational policies and procedures; otherwise, the traveler proceeded to the exit.

Results: (b) (7)(E)
(b) (7)(E)

Recommendations: (b) (5), (b) (7)(E)
(b) (5), (b) (7)(E)

BE-Mobile Device Experiment

Objective: Investigate the feasibility of using a hand-held biographic and biometric (fingerprint) capture device to support exit processing and law enforcement operations. Collect data to improve the understanding of in-scope outbound passenger population and outbound operations.

Description/Scenario: (b) (7)(E)
(b) (7)(E)

(b) (7)(E)

[Redacted text block]

Results:

(b) (7)(E)

[Redacted text block]

Recommendation:

(b) (5), (b) (7)(E)

(b) (5), (b) (7)(E)

[Redacted text block]

DIST Operational and Equipment Summary

Objective: The objective of the Departure Information System Test is to apply facial biometric identification in an air exit environment through a process of Photo Gallery Preparation, Live Photo Capture and Matching, and Post Departure Analysis of Match Scores.

Description/Scenario:

The Departure Information System Test (DIST) consists of a Pre-departure, Departure and Post-Departure process. Pre-departure begins with a photo retrieval to prepare the face matching gallery for passengers on the flight; passenger data is used to generate queries against multiple CBP, DHS and other photo sources. As multiple photos may be found for each potential passenger, each retrieved photo undergoes a template extraction process. About one hour prior to the flight, all successful templates are downloaded and enrolled to the local application gallery. Not all passengers will be in the gallery due to late arrivals and lack of photos for some travelers. In addition, the gallery may contain templates for passengers who do not board. The departure process is a facial capture scenario with the aid of a CBPO or assistant, and passenger face images are captured and matched against the gallery. An attendant scans the passenger boarding pass, which triggers a face finding and photo capture process. In some cases, the passenger may be directed to scan their own boarding pass. The

(b) (7)(E)
[Redacted]

(b) (7) (E)

Results:

(b) (7)(E)
[Redacted]

Recommendation:

(b)(5), (b)(7)(E)
[Redacted]

Section 6: Recommended Alternative and Rationale

(b)(5), (b)(7)(E)

[Redacted text block containing approximately 18 lines of blacked-out content]

APPENDIX A
Acronyms

ADE	Acquisition Decision Event
ADIS	Arrival Departure Information System
AEER	Air Entry/Exit Re-engineering
AoA	Analysis of Alternatives
AoE	Analysis of Experiments
APC	Automated Passport Control
APIS	Advanced Passenger Information System
BE	Biometric Exit
BEMA	Biometric Exit Mobile Application
BTT	Biometric Transaction Terminal
CBP	U.S. Customs and Border Protection
CBPOs	CBP Officers
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DIST	Departure Information System Test
DOTMLPF/R/G/S	Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Regulations/Grants/Standards
EWI	Entry Without Inspection
EXT	Entry Exit Transformation
FAR	False Accept Rate
FIS	Federal Inspection Service
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FOUO	For Official Use Only
FPIR	False Positive Identification Rate
FRR	False Reject Rate
FTA	Failure to Acquire
HART	Homeland Advanced Recognition Technology
IAD	Dulles International Airport
IDENT	Automated Biometric Identification System
ILSP	Integrated Logistics Support Plan
IT	Information Technology
LCCE	Lifecycle Cost Estimate
MdTF	Maryland Test Facility
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPC	Mobile Passport Control
MRZ	Machine Readable Zone

~~FOR OFFICIAL USE ONLY~~

MSBM	Mission Support Business Model
(b)(7)(E)	(b)(7)(E)
NIST	National Institute of Standards and Technology
NTC	National Targeting Center
O&M	Operations & Maintenance
OBIM	Office of Biometric Identify Management
OFO	Office of Field Operations
OIT	Office of Information Technology
PAU	Passenger Analysis Unit
Ped Exit	Pedestrian Exit
PII	Personally Identifiable Information
PMO	Program Management Office
POE	Port of Entry
RFID	Radio Frequency Identification
S&T	Science and Technology
SOP	Standard Operating Procedure
TAR	True Accept Rate
TPIR	True Positive Identification Rate
TSA	Transportation Security Agency
TVS	Traveler Verification Service
USB	Universal Serial Bus
USC	United States Citizen
USCIS	United States Citizenship and Immigration Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology



Homeland Security

MEMORANDUM FOR: Mark Borkowski
Component Acquisition Executive
U.S. Customs and Border Protection

FROM: (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) February 26, 2018
Executive Director
Office of Program Accountability and Risk Management

(b)(6), (b)(7)(C) (b)(6), (b)(7)(C) 2/20/18
Director
Program Analysis and Evaluation Division
Office of the Chief Financial Officer

SUBJECT: U.S. Customs and Border Protection Biometric Entry-Exit
Analysis of Experiments Approach

DECISION:

Given the joint approach taken by U.S. Customs and Border Protection (CBP) and the Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM), both the DHS Office of Program Accountability and Risk Management (PARM) and the Office of the Chief Financial Officer Program Analysis and Evaluation Division support the Analysis of Alternatives (AoA) / Analysis of Experiments (AoE) conducted by CBP's Biometric Entry-Exit program, and do not require the program to provide the traditional AoA / Study Plan document.

BACKGROUND:

Per *Instruction 102-01-001, Acquisition Management*, acquisition programs are required to submit an approved AoA / Study Plan in preparation for Acquisition Decision Event 2A approval.

In lieu of the traditional AoA / Study Plan requirement, CBP conducted an AoA/AoE to provide rationale for its decision to use travelers' facial images as the biometric modality to confirm identity. As part of the planning efforts for its biometric entry-exit mission needs, CBP and DHS OBIM worked closely to coordinate functional and technical requirements. Both entities have also been working jointly to develop a roadmap to utilize OBIM's facial matching capabilities.

(b)(5)

For questions regarding the above guidance, contact (b)(6), (b)(7)(C), PARM, at (b)(6), (b)(7)(C) or (b)(6), (b)(7)(C).

Cc:
Chief Financial Officer
Director, Cost Analysis Division
Chair, Joint Requirements Council
Program Manager, CBP Biometric Entry-Exit Program



Department of Homeland Security
Customs and Border Protection (CBP)

Biometric Entry-Exit Life Cycle Cost Estimate Documentation

Version 2.0

October 9, 2019

Submitted by:	(b)(6), (b)(7)(C) Program Manager	10/16/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Program Acquisition Executive	10/19/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Lead Business Authority	10/16/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Component Chief Financial Officer	8 Nov 19 Date
Endorsed by:	(b)(6), (b)(7)(C) Component Acquisition Executive	9 Nov 19 Date
Endorsed by:	(b)(6), (b)(7)(C) DHS Cost Analysis Division	12/6/19 Date
Approved by:	(b)(6), (b)(7)(C) DHS Chief Financial Officer	12/9/19 Date

Executive Summary

The Biometric Entry-Exit Program's goal is to verify the traveler's identity upon entry into, and departure from, the United States. The design of the Biometric Entry-Exit Program is not limited to collecting biometric information from a departing passenger; the system must also support efforts to ensure that the passenger actually departs from the United States. Customs and Border Protection's (CBP's) first deployed biometric exit capabilities were in the air environment. This required the deployment of a biometric exit solution at or near the departure gate to provide the highest assurance of traveler departure. Working in partnership with the air travel industry, CBP is leading the transformation of air travel using biometrics as the key to enhancing security and unlocking benefits that dramatically improve the entire traveler experience. CBP has reengineered data flows and data systems to pre-stage biometrics data throughout the travel process.

CBP has partnered with airlines, airports, and the Transportation Security Administration (TSA) to build a device independent, vendor neutral, back-end system called the Traveler Verification Service (TVS). This system allows for private sector investment in front end camera technology and network infrastructure, such as self-service baggage drop off kiosks, facial recognition self-boarding gates, and other equipment. This service will ultimately enable a biometric-based entry/exit system to provide significant benefits to air travel partners, in addition to establishing a biometric air exit system. TVS will also support future biometric deployments in the land and sea environments and throughout the traveler continuum. Figure 1 shows the different environments and touchpoints that will interact with TVS.

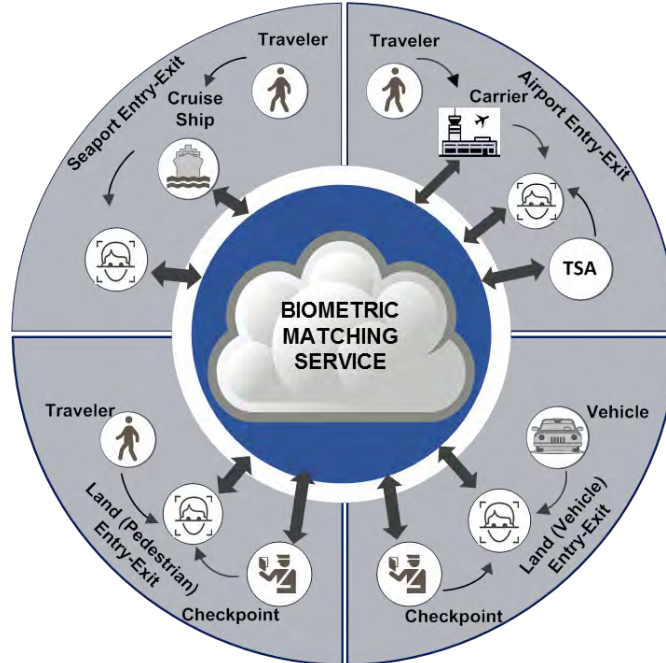


Figure 1: TVS Support Across Environments

Biometric Entry-Exit LCCE Documentation

This Life Cycle Cost Estimate (LCCE) describes the investment and sustainment costs required to support the Biometric Entry-Exit Program. The scope of this LCCE encompasses all activities directly funded by the Biometric Entry-Exit Program (through fee funds or appropriated funds) as well as non-program funded activities that directly support the program. This LCCE represents an update to the approved 2017 LCCE in support of the requirement to update the Biometric Entry-Exit Program Life Cycle Cost Estimate (LCCE) per Department of Homeland Security (DHS) Acquisition and Capital Planning and Investment Control (CPIC) guidance as well as the DHS requirement for annual LCCE update¹. (b)(5)

(b)(5)

Table 1 shows a high-level summary of the LCCE in base year 2017 dollars (BY 17\$), then-year dollars (TY \$), and TY risk-adjusted dollars (TY\$ 50% C.L.). These numbers reflect the total cost of Biometric Entry Exit in the air environment, in addition to the cost to develop and maintain the Sea and Land environments.

Table 1: LCCE High Level Summary

Biometric Entry-Exit Cost Summary	
BY17 \$K	
Total	\$ 1,412,523
PC&I	\$ 361,576
O&S	\$1,050,947
TY \$K	
Total	\$1,622,200
PC&I	\$374,434
O&S	\$1,247,767
TY \$K 50% C.L.	
Total	\$1,830,783
PC&I	\$413,465
O&S	\$1,417,318

¹ DHS DUSM Memorandum. *Annual Cost Estimates*. 11 January 2016

Table of Contents

1.0 Introduction.....6

1.1 Estimate Scope..... 7

1.2 Ground Rules and Assumptions 7

 1.2.1 Program Schedule 7

 1.2.2 Entry-Exit Infrastructure 8

 1.2.3 Work Breakdown Structure 9

 1.2.4 Sunk Costs 9

 1.2.5 Service Delivery Requirements..... 10

 1.2.6 Base Year..... 10

 1.2.7 Land and Sea Environments 11

2.0 Cost Estimating Results.....12

2.1 Investment (PC&I) 12

 2.1.1 Program/Project Management (WBS 1.1.1) 12

 2.1.2 Backend Matching Algorithm (WBS 1.1.6.1)..... 13

 2.1.3 Entry Device Deployment (WBS 1.1.9.2) 13

 2.1.4 Technology and Innovation – Program Funded (WBS 1.1.12.2)..... 15

 2.1.5 Application Implementation (WBS 1.1.9.5) 17

 2.1.6 System Development (WBS 1.1.4) 17

2.2 Operations and Support (O&S)..... 17

 2.2.1 Traveler Verification System (TVS) O&S (WBS 2.1.7.1) 18

 2.2.2 Network Maintenance – Data Center (WBS 2.1.6.4) 18

 2.2.3 Technology and Innovation – O&S (WBS 2.1.12.1)..... 19

 2.2.4 Program Management (WBS 2.1.1)..... 20

 2.2.5 Application O&S (WBS 2.1.6.5) 20

2.3 Summary of Results 21

3.0 Risk and Uncertainty.....27

4.0 Sensitivity Analysis.....31

5.0 Acquisition Program Baseline (APB) Analysis33

6.0 Affordability Analysis35

7.0 Track to Prior LCCE36

Biometric Entry-Exit LCCE Documentation

Table 1: LCCE High Level Summary 3

Table 2: Airports Requiring Device and Network Upgrades 9

Table 3: FY19 OIT SDR..... 10

Table 4: Survey and Design Per Site (TY19\$)..... 13

Table 5: Air Entry Equipment and Labor Per Lane (TY19\$) 14

Table 6: Site/Lane List for Air Entry..... 14

Table 7: VPC 2.0 Development (TY19\$)..... 15

Table 8: Simplified Arrival Development and O&M (TY19\$)..... 15

Table 9: Pedestrian Entry Equipment and Labor Per Lane (TY19\$)..... 16

Table 10: Site/Lane List for Land Technical Demonstrations 16

Table 11: Maintenance Costs for Data Centers (TY19\$)..... 18

Table 12: Pedestrian Lane Equipment Maintenance (TY19\$)..... 19

Table 13: TPAC O&M (TY19\$)..... 20

Table 14: Total Cost Summary (TY\$K) 21

Table 15: Total WBS Phased Cost (TY\$K) 22

Table 16: Total WBS Phased Cost (TY\$K 50% C.L.) 24

Table 17: Risk Bounds for Cost Inputs 27

Table 18: Summary of Previous Program Cost Baseline 33

Table 19: Program Cost Baseline for ADE-3 34

Table 20: Analysis of Program Affordability (TY\$K 50% C.L.)..... 35

Table 21: Track to Prior LCCE 37

Figure 1: TVS Support Across Environments 2

Figure 2: TVS Support Across Environments 7

Figure 3: High Level Milestone Schedule..... 8

Figure 4: Air PC&I Pareto Chart (TY\$ 50% C.L.)..... 12

Figure 5: Air O&S Pareto Chart (TY\$ 50% C.L.)..... 18

Figure 6: Grand Total S-Curve 29

Figure 7: PC&I S-Curve 29

Figure 8: O&S S-Curve 30

Figure 9: PC&I Tornado Chart..... 32

Figure 10: O&S Tornado Chart..... 32

1.0 Introduction

The primary mission of the U.S. Customs and Border Protection (CBP) agency 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. Part of this mission is to enforce U.S. immigration laws. A key aspect of U.S. immigration laws is that most foreign nationals enter as a "nonimmigrant" or on a temporary basis with a fixed period of admission time, and are required to depart the United States before that admission time expires. In order to effectively enforce U.S. immigration law, CBP must have the ability to 1) record departures of foreign nationals from the United States and 2) do so in a way that provides the highest assurance of travelers' identity. If CBP is unable to determine if and when foreign nationals depart from the United States, its ability to enforce a major piece of existing immigration law is limited.² The Biometric Entry-Exit Program's goal is to verify the traveler's identity upon entry into, and departure from, the United States. The design of a Biometric Entry-Exit solution is not limited to collecting biometric information from a departing passenger; the system must also support efforts to ensure that the passenger actually departs from the United States.

CBP's first deployed biometric exit capabilities were in the air environment. This required the deployment of a biometric exit solution at or near the departure gate to provide the highest assurance of traveler departure. Although the initial focus of the Biometric Entry-Exit Program is implementation in the air environment, the program plans to also cover biometric entry-exit for the land and sea environments. Working in partnership with the air travel industry, CBP is leading the transformation of air travel using biometrics as the key to enhancing security and unlocking benefits that dramatically improve the entire traveler experience. CBP has reengineered data flows and data systems to pre-stage biometrics data throughout the travel process.

CBP uses the traveler's face as the primary way of identifying the traveler and facilitating their entry to and exit from the United States, while simultaneously checking fingerprints of non-US citizens against watch lists. This creates an opportunity for CBP to transform air travel by enabling all parties in the travel system to match traveler data via biometrics, thus addressing CBP's border security mandate and streamlining the entire traveler experience.

The CBP approach uses biometrics to streamline passenger processes throughout the air travel continuum, and will provide airport and airlines with the opportunity to validate identities against DHS information systems. CBP has partnered with airlines, airports, and the Transportation Security Administration (TSA) to build a device independent, vendor neutral, back-end system called the Traveler Verification Service (TVS). This system allows for private sector investment in front end camera technology and network infrastructure, such as self-service baggage drop off kiosks, facial recognition self-boarding gates, and other equipment. This service will ultimately enable a biometric-based entry/exit system to provide significant benefits to air travel partners, in addition to establishing a biometric air exit system. TVS will also support future biometric deployments in the land and sea environments and throughout the traveler continuum.

Figure 2 shows the different environments and touchpoints that will interact with TVS.

² Standard Bio Entry-Exit Program Language

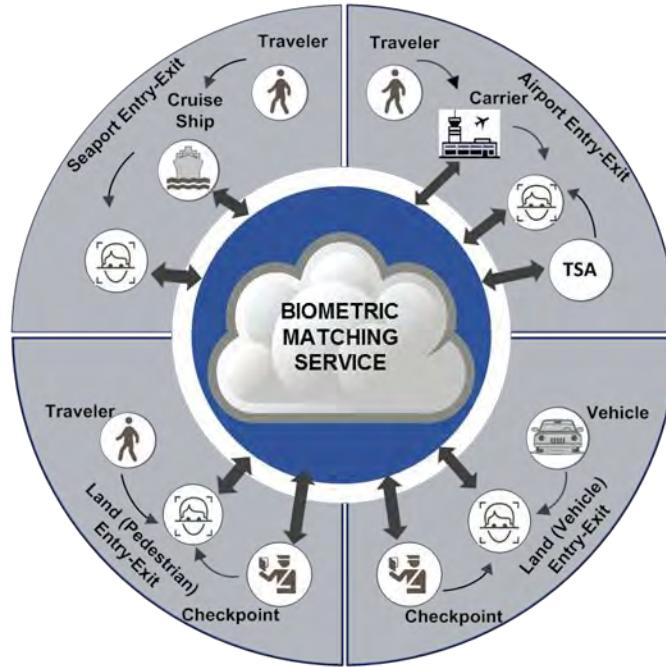


Figure 2: TVS Support Across Environments

1.1 Estimate Scope

The time frame of this estimate ranges from fiscal year 2014 (FY14) through FY31 which captures the sunk costs associated with the program as well as all in-scope program investment and sustainment.

The scope of this LCCE encompasses all activities directly funded by the Biometric Entry-Exit Program (through fee funds or appropriated funds) as well as costs that can be directly attributed to the program. These costs include system development efforts, hardware/software procurement, IT infrastructure, and Office of Field Operations (OFO) and Office of Information Technology (OIT) staff that support the development and management of the Biometric Entry-Exit Program. The scope does not include the cost of CBP officers that enforce the program, along with other CBP initiatives at points of entry and exit. This iteration of the LCCE is an update to the original estimate and includes: FY17 & FY18 actuals, data from the FY19 OIT SDR, and updated key programmatic assumptions primarily in the Air phase. (b)(5)

(b)(5)

1.2 Ground Rules and Assumptions

1.2.1 Program Schedule

The Biometric Entry-Exit Program officially became a program of record in FY16 although technical demonstrations to support the program started prior. The high-level project schedule in Figure 3 includes timelines for the following categories of events: Air Land & Sea Acquisition Events, Air Acquisition Planning, Land Acquisition Planning, Sea Acquisition Planning, IT

Infrastructure, Site Infrastructure, Operational Support, and Technical Innovation & Demonstrators.

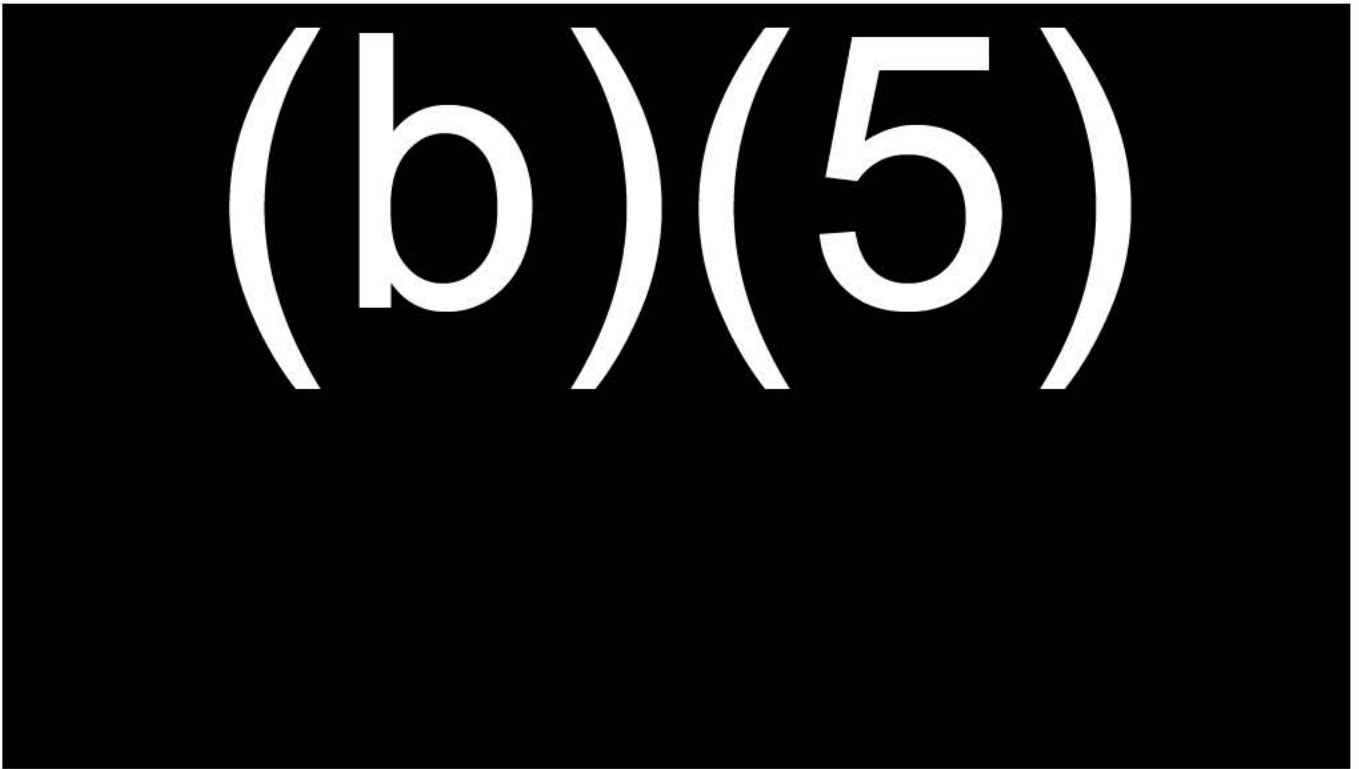


Figure 3: High Level Milestone Schedule

The air segment of the program achieved ADE-1 in Q3 of FY17, received ADE-2A in Q3 of FY18, and ADE-2B in Q1 FY19. (b)(5)

(b)(5)

- (b)(5)
- (b)(5)
- (b)(5)

(b)(5)

1.2.2 Entry-Exit Infrastructure

The Biometric Entry-Exit Program requires some hardware and software components in order to develop, operate, and maintain the program. For points of entry, this includes fingerprint scanners, ePassport readers, touchscreen devices, and facial image cameras at each inbound lane within an airport. (b)(5), (b)(7)(E)

(b)(5), (b)(7)(E) Table 2 shows the

Biometric Entry-Exit LCCE Documentation

airports where upgrades are currently planned, along with the number of lanes that will be upgraded at each airport.

Table 2: Airports Requiring Device and Network Upgrades

Air Deployment Sites		
Sites	Site #	Lanes
(b)(5)	(b)(5), (b)(7)(E)	
Total		(b)(5), (b)(7)(E)

In addition to infrastructure at points of entry, a back-end IT infrastructure from a commercial cloud service provider will be required in order to support the computing and data transfer requirements generated by use of TVS.

(b)(7)(E)

1.2.3 Work Breakdown Structure

The LCCE uses the DHS standard IT WBS published by DHS Cost Analysis Division (CAD) to level three. Beyond level three are program specific cost elements where the actual estimating parameters are located. The Biometric Entry-Exit Program broke out major program elements (Land, Air, Sea) at level two to account for greater visibility into cost contributions of each element to the overall program total. The full WBS can be found in the cost model.

1.2.4 Sunk Costs

Before BEE became a program of record, CBP funded demonstrations to support the development and testing of various biometric capabilities. The costs for the demonstrations are considered sunk and included in the LCCE for completeness. Additionally, all costs for FY17

Biometric Entry-Exit LCCE Documentation

and FY18 have been aligned with actual obligations data provided by CBP and are considered sunk.

1.2.5 Service Delivery Requirements

A significant portion of the costs reflected in this life-cycle estimate are based on funding requests submitted to BEE OFO in the FY19 OIT Service Delivery Requirements (SDR) document. The SDR is a compilation of cost requirements from various directorates within OIT, which include:

- Enterprise Data Management and Engineering Directorate (EDMED)
- Enterprise Networks and Technology Support Directorate (ENTSD)
- Passenger Systems Program Directorate (PSPD)
- Target and Analysis Systems Program Directorate (TASPD)
- Field Support Directorate (FSD)
- Cyber Security Directorate (CSD)

The requirements from the most recent version of the SDR, dated 23 May 2019, are shown in Table 3.

FY19 OIT SDR Funding							
Directorate	Type	FY19	FY20	FY21	FY22	FY23	FY24
CSD	Government Position Cost	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
CSD	O&M	\$ 2,714,466	\$ 2,826,983	\$ 2,940,732	\$ 3,060,869	\$ 3,185,842	\$ 3,133,499
EDMED	O&M	\$ 4,200,000	\$ 4,200,000	\$ 4,200,000	\$ 4,200,000	\$ 4,200,000	\$ 4,200,000
ENTSD	New Investment Cost	\$ 5,000,000	\$ -	\$ -	\$ -	\$ -	\$ -
ENTSD	O&M	\$ 5,790,841	\$ 12,347,285	\$ 12,360,879	\$ 12,375,152	\$ 12,390,140	\$ 12,405,876
FMD	Government Position Cost	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
FMD	New Investment Cost	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
FMD	O&M	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
FSD	O&M	\$ 6,286,525	\$ 2,368,251	\$ 2,368,251	\$ 2,368,251	\$ 2,368,251	\$ 2,318,200
PSPD	Government Position Cost	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
PSPD	New Investment Cost	\$ 17,690,888	\$ -	\$ -	\$ -	\$ -	\$ -
PSPD	O&M	\$ 9,831,129	\$ 16,662,509	\$ 15,484,898	\$ 15,816,467	\$ 16,155,684	\$ 16,502,732
TASPD	O&M	\$ 16,149,912	\$ 16,473,972	\$ 16,768,611	\$ 17,068,839	\$ 17,374,767	\$ 17,686,510
	Total	\$ 67,663,761	\$ 54,879,000	\$ 54,123,371	\$ 54,889,579	\$ 55,674,684	\$ 56,246,818

Table 3: FY19 OIT SDR

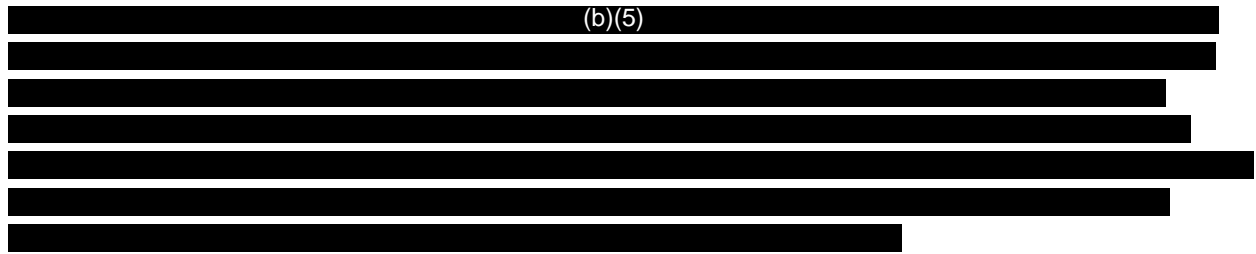
Along with the high-level total requests in the SDR, some directorates provided detailed workbooks that explained how their cost requests broke down at lower levels. Metrics leveraged from these workbooks include equipment and labor costs to install a single entry lane, survey and design costs for each site, and network cabling costs for each site. These metrics, along with some top-level totals, were incorporated into the LCCE.

1.2.6 Base Year

Costs for this LCCE were estimated in base year 2017 dollars (BY17\$) for consistent treatment of inflation. The initial LCCE was developed in BY17\$ and all following LCCEs will convert back to BY17\$ for ease of comparison.

1.2.7 Land and Sea Environments

(b)(5)



2.0 Cost Estimating Results

The following sections show the estimated program costs, ranked by the dollar value, of each cost element for the Biometric Entry-Exit program. Elements that make up the top 80% of investment and 80% of O&S are identified as significant. These cost elements are described in sub sections that provide the estimating methodology, data sources, and assumptions for each element.

2.1 Investment (PC&I)

The Pareto chart in Figure 4 shows the largest PC&I cost elements in the Air environment. The methodologies and assumptions used to estimate the costs of the elements that make up the top 80% of the estimate are documented in the following sections.

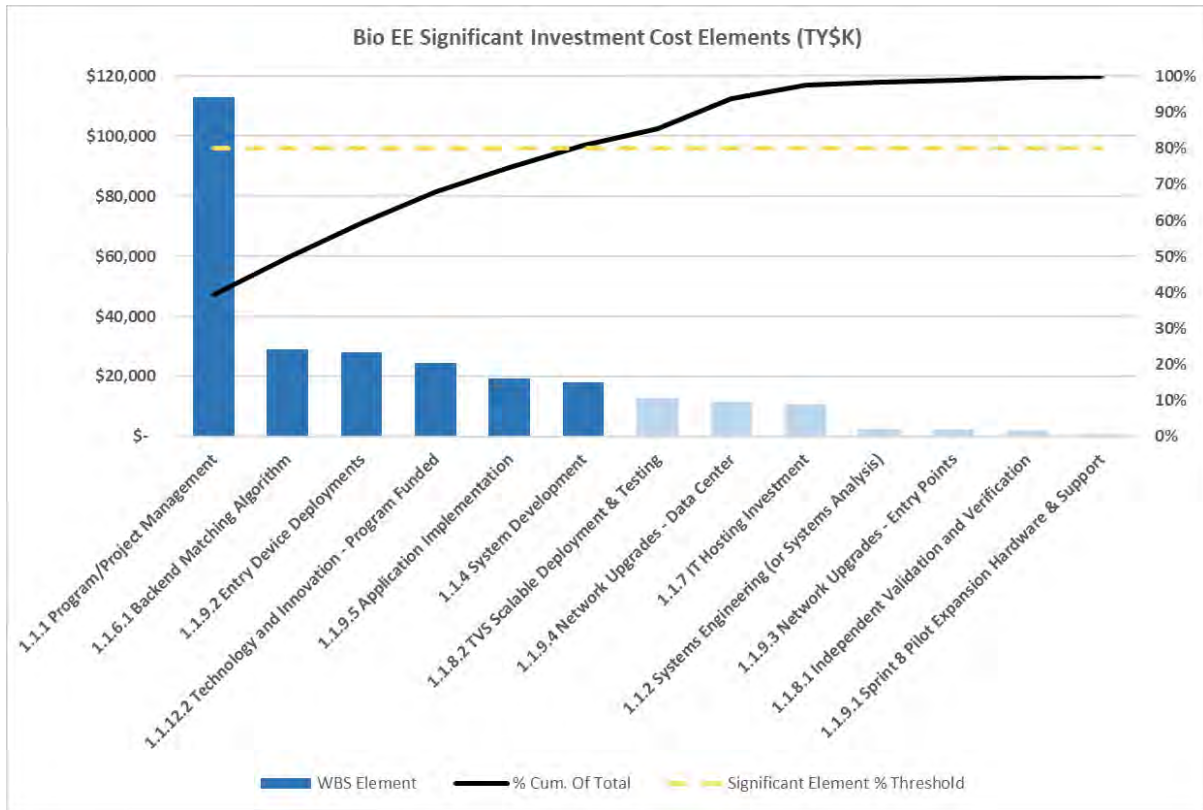


Figure 4: Air PC&I Pareto Chart (TY\$ 50% C.L.)

2.1.1 Program/Project Management (WBS 1.1.1)

This cost element captures the total cost for Acquisition and PM Support for Federal and Contractor support at OFO and Office of Administration (OA) and Federal Staff at OIT, Communication and Outreach & Government Travel cost incurred by the PMO office, and OEA Sim Model Development.

Acquisition and PM Support – Federal (WBS 1.1.1.1): The Biometric Entry-Exit program office developed a comprehensive staffing plan for the program (updated September 2019). OFO and OIT Federal personnel were listed by organization, grade, and function. The staffing

plan estimated current/expected on board staff from FY19 through FOC. Total federal support staffing costs are calculated by applying these quantities to federal labor rates for DC-Baltimore.

Acquisition and PM Support – Contractor (WBS 1.1.1.2): The Biometric Entry-Exit program office developed a comprehensive staffing plan for the program (updated September 2019). Contractor personnel were listed by organization and function. The staffing plan estimated current/expected on board staff from FY19 through FOC. Total contractor support staffing costs are calculated by applying FTEs to labor rates by position pulled from the General Services Administration (GSA) website.

Miscellaneous PM (WBS 1.1.1.3): This element includes Communication and Outreach costs and PMO travel. Communication and Outreach costs are estimated using historical WHTI Communication and outreach costs to develop a factor of communications costs to initial acquisition costs. SME Judgment was used to phase costs throughout PC&I. The phasing assumes 10% of the communications budget was expended in FY17 & FY18, ramps-up to 30% in FY19 & FY20, and ramps down to 20% in FY21 (FOC). Additionally, an average annual PMO travel cost was provided by the Biometric Entry-Exit PMO.

Enterprise Analytics (WBS 1.1.1.4): Costs were estimated by developing an average annual cost based on FY17 and FY18 sunk costs.

2.1.2 Backend Matching Algorithm (WBS 1.1.6.1)



2.1.3 Entry Device Deployment (WBS 1.1.9.2)

Entry Device Deployment includes material/ODCs, labor, and survey/design costs for each new air entry deployment. Costs for FY18 and prior are based on program office spend plan obligations. Costs for FY19 and forward are based on an engineering build-up that uses the following equation:

$$\text{Infrastructure Cost} = (\text{Per Site Cost} * \text{Site Quantity}) + (\text{Per Lane Cost} * \text{Lane Quantity})$$

Per-site costs can be found in Table 4, while per-lane costs for air entry are shown in Table 5. Site and lane quantities for the air environment can be found in Table 6. Costs were provided by PSPD in their PSPD SDR Detail workbook, while the site list was acquired from the OFO.

Table 4: Survey and Design Per Site (TY19\$)

Per Site Cost	
Description	Cost
Per Site Survey	\$ 16,950
Per Site Design	\$ 22,500
Total Per Site	\$ 39,450

Biometric Entry-Exit LCCE Documentation

Table 5: Air Entry Equipment and Labor Per Lane (TY19\$)

Per Lane Cost	
Description	Cost
(b)(7)(E)	\$ 1,091
	\$ 203
	\$ 100
	\$ 560
	\$ 1,765
	\$ 838
	\$ 300
	\$ 165
	\$ 306
	\$ 73
Per Lane Equipment	\$ 5,401
Per Lane Labor	\$ 3,529
Total Per Lane	\$ 8,930

Table 6: Site/Lane List for Air Entry

Air Deployment Sites FY19				
Sites	Site #	Lanes		
Detroit	(b)(7)(E)	(b)(7)(E)		
Atlanta				
IAD				
Orlando				
Houston Hobby				
San Jose				
San Francisco				
Dallas Fort Worth				
Los Angeles				
JFK				
Total			(b)(7)(E)	(b)(7)(E)
FY20				
Sites	Site #	Lanes		
(b)(5)	(b)(7)(E)	(b)(7)(E)		
Total	(b)(7)(E)	(b)(7)(E)		
Post FY20				
Sites	Site #	Lanes		
(b)(5)	(b)(7)(E)	(b)(7)(E)		
Total	(b)(7)(E)	(b)(7)(E)		

2.1.4 Technology and Innovation – Program Funded (WBS 1.1.12.2)

Includes all pre-FOC costs, including both software and hardware costs, incurred for technical demonstrations in the land environment. Software costs consist of the costs of two applications: Vehicle Primary Client (VPC), and Simplified Arrival (SA) in the land environment. VPC development costs are shown in Table 7, while software development costs for SA are shown in Table 8. It was assumed, based on SME judgment, that 25% of the total cost of SA was in support of the land environment. A Contract Fixed Fee of 9% was added to these application costs, which were provided by PSPD in the PSPD SDR Detail workbook.

Table 7: VPC 2.0 Development (TY19\$)

Vehicle Primary Client 2.0 - 15 FTE		
	Hours	Cost
Project Manager	186	\$29,239
Senior SME	1,491	\$229,818
Software Engineer	6,873	\$652,699
Software Engineer Junior	75	\$6,002
Software Engineer Senior	6,021	\$835,715
Systems Analyst	2,610	\$217,670
Systems Architect	37	\$6,032
Systems Engineer	37	\$3,001
Systems Engineer Senior	1,444	\$232,085
Technical Manager	2,423	\$323,678
Technical Project Manager	56	\$7,173
Test Engineer	932	\$86,348
Test Engineer Senior	5,965	\$697,290
VPC 2.0 Total	28,151	\$3,326,749

Table 8: Simplified Arrival Development and O&M (TY19\$)

Simplified Arrival - 34 FTE		
	Hours	Cost
Contract Administrator	153	\$12,830
Database Administrator	746	\$95,394
Project Control Specialist	357	\$25,672
Project Manager	746	\$116,957
Senior SME	4,101	\$683,387
Software Engineer	4,596	\$458,958
Software Engineer Junior	9,670	\$737,138
Software Engineer Senior	18,105	\$2,325,409
Systems Analyst	2,982	\$399,793
Systems Analyst Senior	1,864	\$268,407
Systems Architect	2,180	\$351,508
Systems Engineer	1,268	\$102,029
Systems Engineer Senior	8,761	\$1,103,623
Technical Manager	3,169	\$422,297
Technical Project Manager	1,249	\$160,201
Test Engineer	932	\$86,348

Biometric Entry-Exit LCCE Documentation

Test Engineer Senior	3,355	\$363,506
Shared Cost		\$366,327
SA Total		\$8,079,784
Development Total		\$2,778,471
Enhancement Total		\$2,398,402
O&M Total		\$2,902,911

The infrastructure required to support these applications was calculated by applying per-site survey and design costs, shown in Table 4, and per-lane pedestrian equipment and labor costs, shown in Table 9 to site and lane quantities shown in Table 10.

Table 9: Pedestrian Entry Equipment and Labor Per Lane (TY19\$)

Per Lane Cost	
Description	Cost
(b)(7)(E)	\$ 1,091
	\$ 203
	\$ 100
	\$ 560
	\$ 4,000
	\$ 300
	\$ 375
	\$ -
	\$ 511
	Per Lane Equipment
Per Lane Labor	\$ 9,096
Total Per Lane	\$ 16,236

Table 10: Site/Lane List for Land Technical Demonstrations

Land Demo Deployment Sites/Lanes		
FY19		
Sites	Site #	Lanes
San Ysidro West	(b)(7)(E)	
San Ysidro East		
Otay Mesa		
Cross Border Express		
Tecate		
El Paso (Paso Del Norte)		
El Paso (Bridge of the Americas)		
El Paso (Ysleta)		
Laredo (Convent St.)		
Lincoln-Juarez Bridge		
FY19 Total		
FY20		
Sites	Site #	Lanes
(b)(5)	(b)(7)(E)	

Biometric Entry-Exit LCCE Documentation

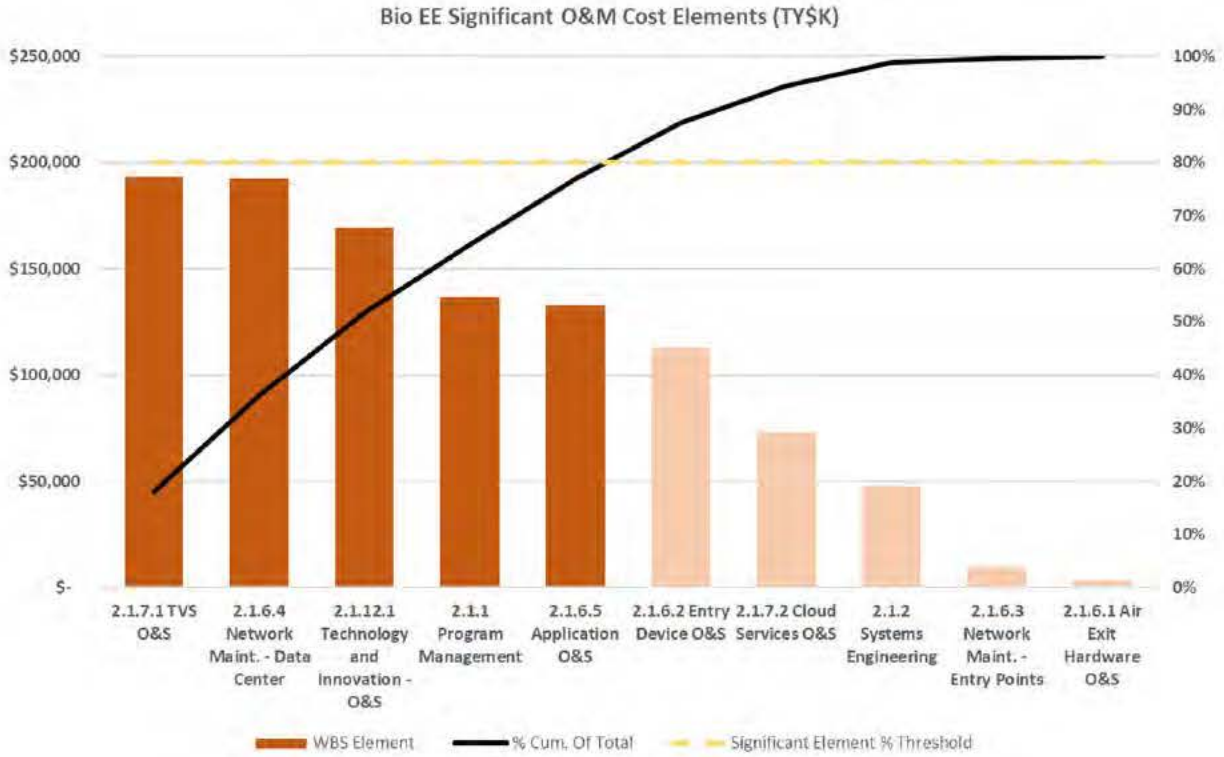


Figure 5: Air O&S Pareto Chart (TY\$ 50% C.L.)

2.2.1 Traveler Verification System (TVS) O&S (WBS 2.1.7.1)

Includes the cost of adaptive maintenance for TVS in the air environment. (b)(5)

(b)(5)

2.2.2 Network Maintenance – Data Center (WBS 2.1.6.4)

Includes recurring costs for infrastructure and services at the data centers maintained by the Enterprise Network Technology and Support Directorate (ENTSD). Some of these costs are BEE-specific, while others are paid as a percentage of the total cost of supporting multiple CBP programs. A list of these charges, provided by ENTSD is shown in Table 11.

Table 11: Maintenance Costs for Data Centers (TY19\$)

Description	FY19	FY20	FY21	FY22	FY23	FY24
(b)(7)(E) (b)(5), (b)(7)(E)						

Biometric Entry-Exit LCCE Documentation

Description	FY19	FY20	FY21	FY22	FY23	FY24
(b)(7)(E) (b)(5), (b)(7)(E)						

2.2.3 Technology and Innovation – O&S (WBS 2.1.12.1)

This cost element includes the cost of maintaining all software and hardware deployed through technical demonstrations in the land environment. (b)(7)(E)

(b)(7)(E)

Hardware costs consists of maintenance for lane equipment and network infrastructure at points of entry. (b)(7)(E)

(b)(7)(E)

Table 12: Pedestrian Lane Equipment Maintenance (TY19\$)
Pedestrian Entry Pilot O&M Per Year

Pedestrian Entry Pilot O&M Per Year	
(b)(7)(E)	
Total O&M Cost per Lane Per Year	\$3,798.44

Network maintenance is performed by the Field Support Directorate (FSD), and includes the cost of installing and refreshing switches and cables. Installation costs are calculated by deriving a per-site cost which is applied to site quantities provided by the PMO. (b)(7)(E)

(b)(7)(E)

2.2.4 Program Management (WBS 2.1.1)

Acquisition and PM Support – Federal (WBS 1.1.1.1): The Biometric Entry-Exit program office developed a comprehensive staffing plan for the program (updated September 2019). OFO and OIT Federal personnel were listed by organization, grade, and function. (b)(5)

(b)(5) Total federal support staffing costs are calculated by applying these quantities to federal labor rates for DC-Baltimore.

Acquisition and PM Support – Contractor (WBS 1.1.1.2): The Biometric Entry-Exit program office developed a comprehensive staffing plan for the program (updated September 2019). Contractor personnel were listed by organization and function. (b)(5)

(b)(5) Total contractor support staffing costs are calculated by applying FTEs to labor rates by position pulled from the General Services Administration (GSA) website.

Miscellaneous PM (WBS 2.1.1.3): This element includes annual PMO travel costs provided by the Biometric Entry-Exit PMO.

Enterprise Analytics (WBS 2.1.1.4): (b)(5)

2.2.5 Application O&S (WBS 2.1.6.5)

Includes the cost of maintaining and enhancing Simplified Arrival (SA) for the air environment, as well as Traveler Primary Arrival Client (TPAC), which is the primary passenger screening module used to process, document, and confirm the identity of international travelers at air and sea ports of entry. Enhancement and O&M costs for SA can be found in Table 8 while the breakdown of labor for TPAC is shown in Table 13. A 9% contract fixed fee, along with costs for shared services, site surveys and travel, are also included in this element.

Projected costs for this element for FY19-24 were provided by PSPD in the PSPD OIT SDR Detail workbook; these costs were extrapolated forward.

Table 13: TPAC O&M (TY19\$)

Traveler Primary Arrival Client - 7 FTEs		
	Hours	Cost
Project Manager	186	\$29,239
Software Engineer	629	\$61,149
Software Engineer Junior	952	\$61,741
Software Engineer Senior	1,864	\$235,878
Systems Engineer Senior	1,864	\$205,591
Technical Manager	2,251	\$312,540
Technical Project Manager	932	\$112,017
Test Engineer	1,864	\$136,513
Test Engineer Senior	1,864	\$196,034
TPAC Total	12,406	\$1,350,703

2.3 Summary of Results

Table 14 shows the estimated life cycle results in then year dollars (TY\$) for both the point estimate and the risk adjusted estimate. The Point Estimate refers to costs that have not been adjusted for risk. Risk Adjusted TY\$ refers to the results of Monte Carlo Simulations and are presented for the 50% confidence level. This view also shows the costs for each lower-level program component. Table 15 and Table 16 show the point estimate and risk-adjusted estimate phased over time.

Table 14: Total Cost Summary (TY\$K)

WBS Number	Cost Element	Point Estimate	50% Estimate			
	Total LCCE Cost	1,622,200	1,830,783			
1.0	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)			
1.1						
1.1.1						
1.1.2						
1.1.3						
1.1.4						
1.1.5						
1.1.6						
1.1.7						
1.1.8						
1.1.9						
1.1.10						
1.1.11						
1.1.12						
1.2	(b)(7)(E)	(b)(7)(E)	(b)(7)(E)			
1.3						
2.0						
				Operations & Sustainment	29,119	29,119
2.1				(b)(7)(E)	(b)(7)(E)	(b)(7)(E)
2.1.1						
2.1.2						
2.1.3						
2.1.4						
2.1.5						
2.1.6						
2.1.7						
2.1.8						
2.1.9						
2.1.10						
2.1.11						
2.1.12						
2.2						
2.3						

Biometric Entry-Exit LCCE Documentation

Table 15: Total WBS Phased Cost (TY\$K)

#	WBS Element	Prior (FY14 - 17)	FY18	FY19	FY20	FY21	FY22	FY23	FY24	To Complete (FY25-31)	Total	
	Total LCCE	85,120	80,314	101,775	137,747	119,352	87,807	89,378	106,851	813,857	1,622,200	
1.0	(b)(5), (b)(7)(E)											
1.1												
1.1.1												
1.1.1.1												
1.1.1.2												
1.1.1.3												
1.1.1.4												
1.1.2												
1.1.2.1												
1.1.2.2												
1.1.3												
1.1.4												
1.1.4.1												
1.1.4.2												
1.1.5												
1.1.6												
1.1.6.1												
1.1.7		(b)(5), (b)(7)(E)										
1.1.7.1												
1.1.7.2												
1.1.8												
1.1.8.1												
1.1.8.2												
1.1.9												
1.1.9.1												
1.1.9.2												
1.1.9.3												
1.1.9.4												
1.1.9.5												
1.1.10												

Biometric Entry-Exit LCCE Documentation

#	WBS Element	Prior (FY14 - 17)	FY18	FY19	FY20	FY21	FY22	FY23	FY24	To Complete (FY25-31)	Total
1.1.11	(b)(5), (b)(7)(E)										
1.1.12											
1.1.12.1	(b)(5), (b)(7)(E)										
1.1.12.2											
1.2	(b)(5), (b)(7)(E)										
1.3											
2.0											
2.1											
2.1.1											
2.1.1.1											
2.1.1.2											
2.1.1.3											
2.1.1.4											
2.1.2											
2.1.2.1											
2.1.2.2											
2.1.3											
2.1.4											
2.1.5											
2.1.6											
2.1.6.1											
2.1.6.2											
2.1.6.3											
2.1.6.4											
2.1.6.5											
2.1.7											
2.1.7.1											
2.1.7.2											
2.1.7.3											
2.1.8											
2.1.9											
2.1.10											

Biometric Entry-Exit LCCE Documentation

#	WBS Element	Prior (FY14 - 17)	FY18	FY19	FY20	FY21	FY22	FY23	FY24	To Complete (FY25-31)	Total
2.1.11	(b)(5), (b)(7)(E)										
2.1.12											
2.1.12.1											
2.2											
2.3											

Table 16: Total WBS Phased Cost (TY\$K 50% C.L.)

#	WBS Element	Prior (2014 - 2017)	2018	2019	2020	2021	2022	2023	2024	Future (2025 - 2031)	Total
	Total LCCE	85,120	80,314	116,404	160,570	136,258	98,936	100,691	122,115	930,375	1,830,783
1.0	(b)(5), (b)(7)(E)										
1.1											
1.1.1											
1.1.1.1											
1.1.1.2											
1.1.1.3											
1.1.1.4											
1.1.2											
1.1.2.1											
1.1.2.2											
1.1.3											
1.1.4											
1.1.4.1											
1.1.4.2											
1.1.5											
1.1.6											
1.1.6.1											
1.1.7											
1.1.7.1											
1.1.7.2											
1.1.8											
1.1.8.1											

Biometric Entry-Exit LCCE Documentation

#	WBS Element	Prior (2014 - 2017)	2018	2019	2020	2021	2022	2023	2024	Future (2025 - 2031)	Total
1.1.8.2	(b)(5), (b)(7)(E)										
1.1.9											
1.1.9.1											
1.1.9.2											
1.1.9.3											
1.1.9.4											
1.1.9.5											
1.1.10											
1.1.11											
1.1.12											
1.1.12.1											
1.1.12.2											
1.2											
1.3											
2.0	(b)(5), (b)(7)(E)										
2.1											
2.1.1											
2.1.1.1											
2.1.1.2											
2.1.1.3											
2.1.1.4											
2.1.2											
2.1.2.1											
2.1.2.2											
2.1.3											
2.1.4											
2.1.5											
2.1.6											
2.1.6.1											
2.1.6.2											
2.1.6.3											
2.1.6.4											

Biometric Entry-Exit LCCE Documentation

#	WBS Element	Prior (2014 - 2017)	2018	2019	2020	2021	2022	2023	2024	Future (2025 - 2031)	Total
2.1.6.5	(b)(5), (b)(7)(E)										
2.1.7											
2.1.7.1											
2.1.7.2											
2.1.7.3											
2.1.8											
2.1.9											
2.1.10											
2.1.11											
2.1.12											
2.1.12.1											
2.2											
2.3											

3.0 Risk and Uncertainty

(b)(7)(E)

Table 17: Risk Bounds for Cost Inputs

Parameter	Low (15%)	Point Estimate	High (85%)	Risk Source / Chosen Distribution
(b)(7)(E)				

(b)(7)(E)

(b) (7) (E)

Biometric Entry-Exit LCCE Documentation

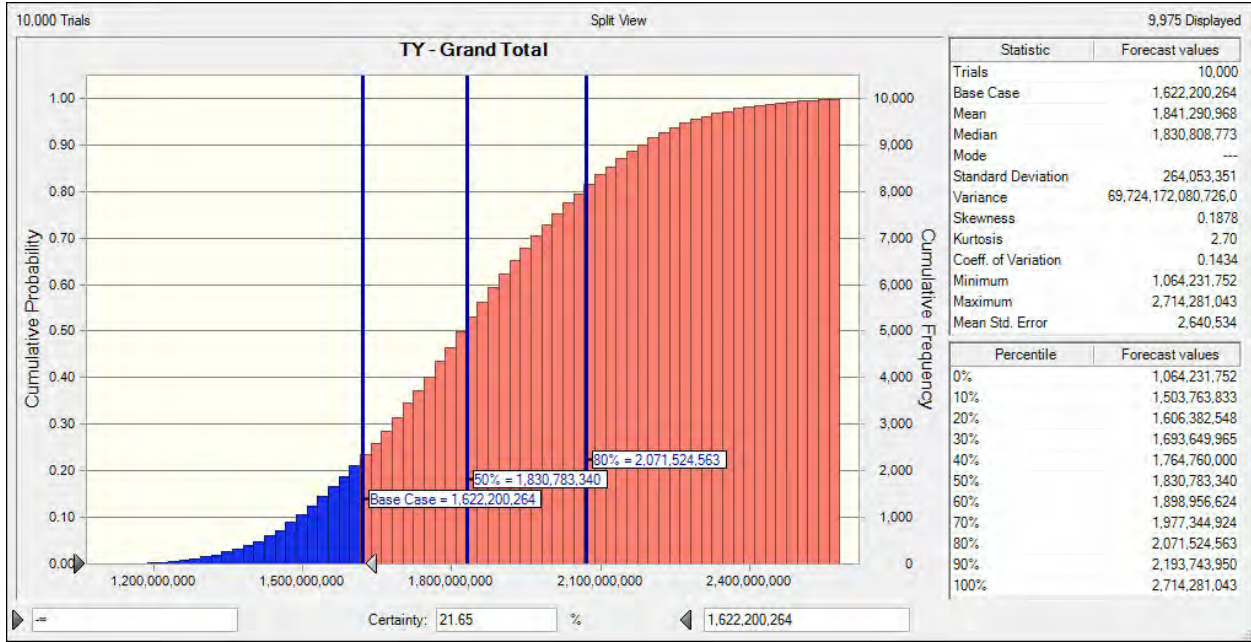


Figure 6: Grand Total S-Curve

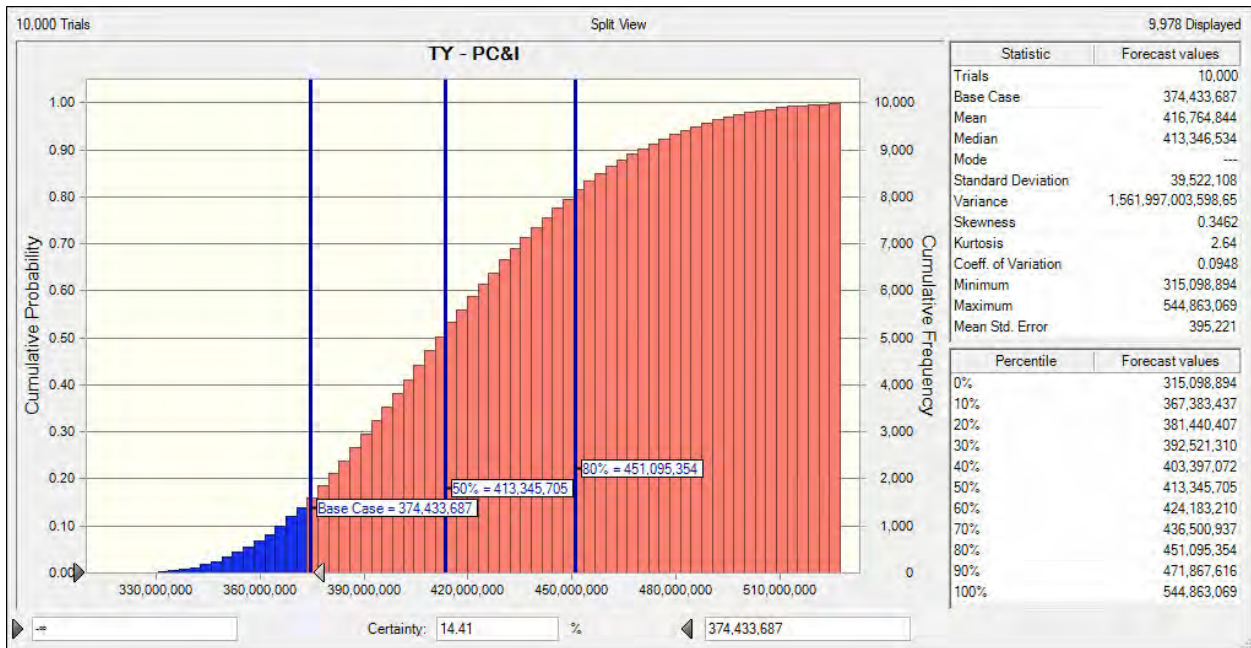


Figure 7: PC&I S-Curve

Biometric Entry-Exit LCCE Documentation

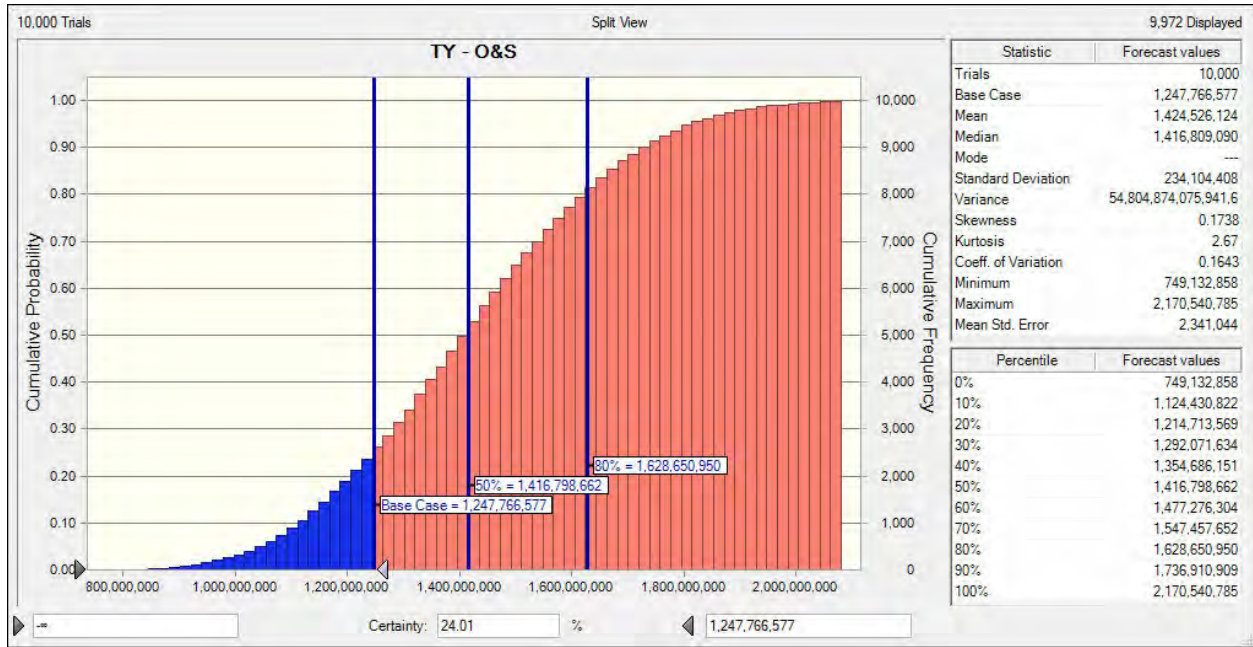


Figure 8: O&S S-Curve

4.0 Sensitivity Analysis

Sensitivity analysis identifies the cost model inputs that have the greatest impact on the overall cost estimate and are often referred to as cost drivers. A sensitivity analysis was conducted by isolating risk inputs and varying them independently between their high and low bounds, one at a time, in order to determine the impacts that each of them could have on program cost. Table 17 in the previous section shows the risk inputs and their high and low bounds.

Figure 9 and Figure 10 show the results of the sensitivity analysis, with the top cost drivers ordered from highest to lowest sensitivity. The width of the bars shows the total LCCE cost by phase when each cost driver is varied between its lower bound and upper bound (corresponding to the x-axis values). The data labels on either side of each bar show the low and high values for that cost driver.

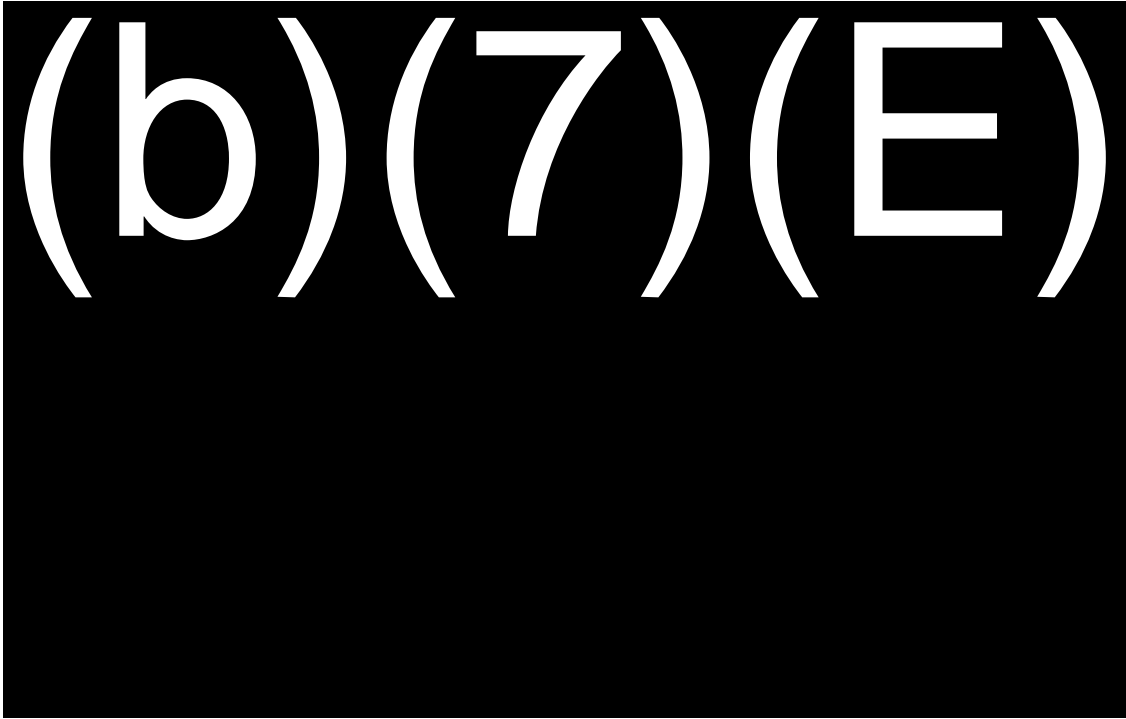


Figure 9: PC&I Tornado Chart

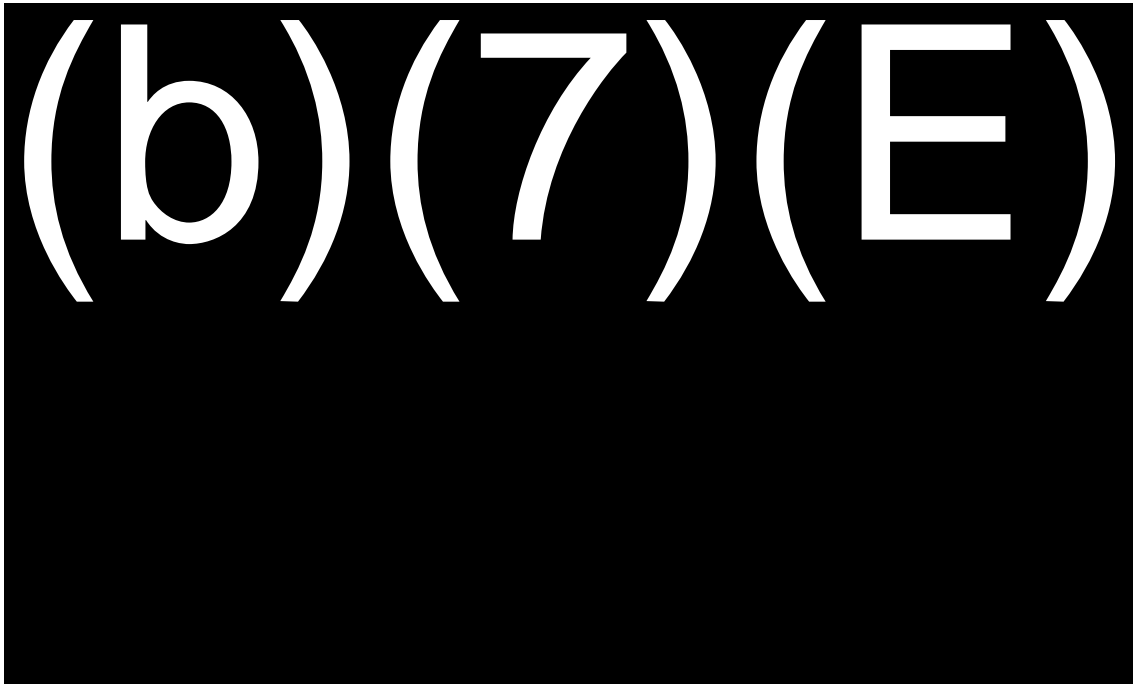


Figure 10: O&S Tornado Chart

5.0 Acquisition Program Baseline (APB) Analysis

The Biometric Entry-Exit program APB was set in 2017 based on the risk-adjusted cost estimate from the last approved LCCE (dated July 2017). Table 18 below shows the threshold and objective by program phase. The threshold was calculated by adding 15% to the objective.

Table 18: Summary of Previous Program Cost Baseline
Biometric Entry-Exit Cost Baseline in Then Year Dollars
(TY\$M 50% CL)

Cost Categories	Baseline Threshold	Baseline Objective
Acquisition (R&D + PC&I)	\$196.7	\$171.0
Operations and Maintenance (O&S)	\$520.1	\$452.3

(b)(5)

(b)(5) The following efforts have been removed from the LCCE since the previous estimate:

- **(b)(7)(E)**
- **(b)(7)(E)**

Meanwhile, the following items have been added:

- **(b)(7)(E)**
- **(b)(7)(E)**
- **(b)(7)(E)**
- **(b)(7)(E)**

Biometric Entry-Exit LCCE Documentation

Since the previous estimate, the costs of several other program elements have increased due to the increasing scope of the program. (b)(5)

(b)(5) As the number of airports serviced has expanded, the program has incurred additional costs in Program Management (1.1.1, 2.1.1), Entry Device Deployments/O&M (1.1.9.2, 2.1.6.2), Network Infrastructure at Entry Points (1.1.9.3, 2.1.6.3), and TVS Deployment/O&M (1.1.8, 2.1.7.1).

Table 19: Program Cost Baseline for ADE-3

Biometric Entry-Exit Cost Baseline (BY17\$M 50% CL)		
Cost Categories	Baseline Threshold	Baseline Objective
Acquisition (R&D + PC&I)	\$252.3	\$219.4
Operations and Maintenance (O&S)	\$833.7	\$724.9
Date Signed		TBD

Biometric Entry-Exit LCCE Documentation

6.0 Affordability Analysis

Table 20: Analysis of Program Affordability (TY\$K 50% C.L)

Summary (50% CL - TY\$K)	Prior (FY14- 17)	FY18	FY19	FY20	FY21	FY22	FY23	FY24	FY25	To Complete (FY26-31)	Total
LCCE TY\$K (50% Confidence Level)											
Acquisition (PC&I)	85,120	80,314	68,035	93,723	63,091	11,537	11,646	0	0	0	413,465
Operations & Maintenance (O&S)	0	0	48,369	66,848	73,167	87,399	89,045	122,115	124,691	805,684	1,417,318
Total	85,120	80,314	116,404	160,570	136,258	98,936	100,691	122,115	124,691	805,684	1,830,783
Adjusted LCCE TY\$K (50% Confidence Level)											
Acquisition (PC&I)	61,540	74,693	35,232	32,316	21,606	0	0	0	0	0	225,386
Operations & Maintenance (O&S)	0	0	40,858	54,513	54,854	64,398	65,582	66,823	68,167	438,854	854,048
Total	61,540	74,693	76,090	86,828	76,460	64,398	65,582	66,823	68,167	438,854	1,079,435
Total Budget Authority TY\$K (FYHSP - Congressional)											
USCIS Fee Funding	140,735	59,522	60,000	61,000	61,000	61,000	61,000	61,000	61,000	427,000	992,257
Surplus / (Shortfall)											
Surplus / (Shortfall)	79,195	(15,171)	(16,090)	(25,828)	(15,460)	(3,398)	(4,582)	(5,823)	(7,167)	(11,854)	(26,178)
Surplus / (Shortfall) with Carry- Over	79,195	64,025	47,935	22,107	6,646	3,248	(1,334)	(7,157)	(14,324)	(26,178)	
Surplus / (Shortfall) with Carry- Over %	129%	86%	63%	25%	9%	5%	-2%	-11%	-21%	-6%	

An Affordability Analysis shown in Table 20 compares the estimated requirement of all activities funded by the Biometric Entry-Exit program (“Adjusted LCCE”) to the available funding for the program.

The requirement accounts only for activities in the air environment and removes all land and sea costs, including the ROMs as well as technical demonstrations captured in Technology and Innovation – Program Funded (1.1.12.2) and Technology and Innovation O&S (2.1.12.1). Additionally, efforts that are within the scope of the program but are funded by outside sources are not captured. This includes federal PM support, captured in Acquisition and PM Support – Federal (1.1.1.1) and Acquisition and PM Support – Federal (2.1.1.1).

Currently the program is funded by USCIS Fee Funding. While collections are less than expected, USCIS has committed to including language in their annual rulemaking review to collect fees on visa extensions. This has the potential to double fee collections for the program

Biometric Entry-Exit LCCE Documentation

in FY21. Additional ways in which the program will address potential annual shortfall are as follows:

- (b)(5)
- (b)(5)
- (b)(5)
- (b)(5)
- (b)(5)

7.0 Track to Prior LCCE

Table 21 below illustrates how the LCCE estimate has changed since the last signed LCCE dated 12 February 2017. As seen below, the total estimate cost of the PC&I phase has increased by 64%. This change has primarily been driven by:

- Program Management (1.1.1) life-cycle cost increase of approximately \$96M TY due to scope increases, including the addition of enterprise analytics.
- System Deployment and Implementation (1.1.9) life-cycle cost increase of approximately \$36M TY to account for to added applications, expanded entry devices and network.
- Other PC&I (1.1.12) life-cycle cost increase of approximately \$11M TY to account for a larger quantity of technical demonstrations than initially planned.
- Biometric Entry-Exit Sea (1.2) life-cycle cost increase of approximately \$11M TY due to improved knowledge of requirements, although this estimate is still a Rough Order of Magnitude (ROM).
- Biometric Entry-Exit Land (1.3) life-cycle cost increase of approximately \$55M due to improved knowledge of requirements, although this estimate is still a ROM.

The total estimated cost of the O&S phase decreased by 18%. This is largely due to Manpower (2.1.4) (TSA and ICE agents at points of entry and exit) being removed from the scope of the estimate. Since these agents are employed independently of the BEE program, it was decided that their salaries should be removed from the estimate in order to more accurately show the BEE-specific cost. While this cost has been removed, other program costs have increased, including:

- Program Management (2.1.1) life-cycle cost increase of approximately \$111M TY due to increased scope of work.
- Systems Engineering (2.1.2) life-cycle cost increase of approximately \$48M TY due to addition of cybersecurity.
- Maintenance and Tech-Refresh (2.1.6) life-cycle cost increase of approximately \$370M TY to provide O&M for added applications, expanded entry devices and network.

Biometric Entry-Exit LCCE Documentation

- Sustaining Support (2.1.7) life-cycle cost increase of approximately \$30M TY due to higher-than expected cost of adaptive maintenance for TVS.
- Other O&S (2.1.12) life-cycle cost increase of approximately \$108M TY to fund O&M for technical demonstrations in the land environment.
- Biometric Entry-Exit Sea (2.2) life-cycle cost increase of approximately \$20M TY due to improved knowledge of requirements, although this estimate is still a ROM.
- Biometric Entry-Exit Land (2.3) life-cycle cost increase of approximately \$156M TY due to improved knowledge of requirements, although this estimate is still a ROM.

Table 21: Track to Prior LCCE

#	Name	Version 1.3	Version 2.0	\$ Change	% Change
	Total LCCE	1,981,451	1,830,783	(150,668)	-8%
1.0	PC&I	251,628	413,465	161,837	64%
1.1	Biometric Entry Exit - Air	190,825	286,641	95,816	50%
1.1.1	Program/Project Management	42,148	112,884	70,736	168%
1.1.2	Systems Engineering	-	2,365	2,365	0%
1.1.3	Business Process Re-engineering	-	-	-	0%
1.1.4	System Development	65,799	18,151	(47,648)	-72%
1.1.5	System Production	-	-	-	0%
1.1.6	COTS/GOTS/GFE Procurement	21,046	29,119	8,072	38%
1.1.7	IT Hosting Investment	10,403	10,695	292	3%
1.1.8	System Level Integration & Test	-	14,584	14,584	0%
1.1.9	System Deployment/Implementation	25,780	62,049	36,269	141%
1.1.10	System Documentation & Related Data	-	-	-	0%
1.1.11	Training	-	-	-	0%
1.1.12	Other PC&I	25,649	36,794	11,145	43%
1.2	Biometric Entry Exit - Sea	25,893	36,712	10,819	42%
1.3	Biometric Entry Exit - Land	34,911	90,113	55,202	158%
2.0	O&S	1,729,823	1,417,318	(312,505)	-18%
2.1	Biometric Entry Exit - Air	1,558,302	1,070,262	(488,039)	-31%
2.1.1	Program/Project Management	26,071	136,579	110,507	424%
2.1.2	Systems Engineering	-	47,633	47,633	0%
2.1.3	Business Process Re-engineering	-	-	-	0%
2.1.4	Manpower	1,076,899	-	(1,076,899)	-100%
2.1.5	Operations	-	-	-	0%
2.1.6	Maintenance & Tech Refresh	80,949	450,616	369,667	457%
2.1.7	Sustaining Support	236,391	266,517	30,126	13%
2.1.8	Continuing System Improvement	64,667	-	(64,667)	-100%
2.1.9	Indirect Support	-	-	-	0%
2.1.10	System Documentation & Related Data	-	-	-	0%
2.1.11	Support Facilities Sustainment & Maintenance	-	-	-	0%
2.1.12	Other O&S	61,064	168,917	107,854	177%
2.2	Biometric Entry Exit – Sea	54,014	73,890	19,876	37%
2.3	Biometric Entry Exit – Land	117,507	273,166	155,659	132%



CCP/PARE 2.0

This is an interactive training guide. When in presentation mode, users can interact with the application by clicking different buttons and elements. Yellow tooltips are provided for further explanation and instruction.

PARE 2.0 as of FY 2020 is a pilot system, not an official system of record. ACE is the official system of record.





TABLE OF CONTENTS

- [3](#) Request Access
- [4](#) The Setup
- [5](#) Basic Features
- [6](#) Login
- [8](#) Primary Queue
- [9](#) Biometric Matching
- [16](#) Enrollment





REQUEST ACCESS TO CBP/PARE 2.0

(b) (7)(E)

- (b) (7)(E)
(b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
[Redacted]

(b) (7)(E)

- (b) (7)(E)
[Redacted]

(b) (7)(E)

- (b) (7)(E)
(b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
[Redacted]
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)



THE SETUP

Screen 1: ACE

Screen 2: CCP/PARE 2.0

(b) (7)(E)(b) (7)(E)

ePassport Reader





BASIC FEATURES

(b) (7)(E)

(b)(6), (b)(7)(C), (b)(7)(E)

(b) (7)(E)

(b) (7)(E)

Withheld in Full Pursuant to, (b)(7)(E)

Withheld in Full Pursuant to, (b)(7)(E)

Withheld in Full Pursuant to, (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

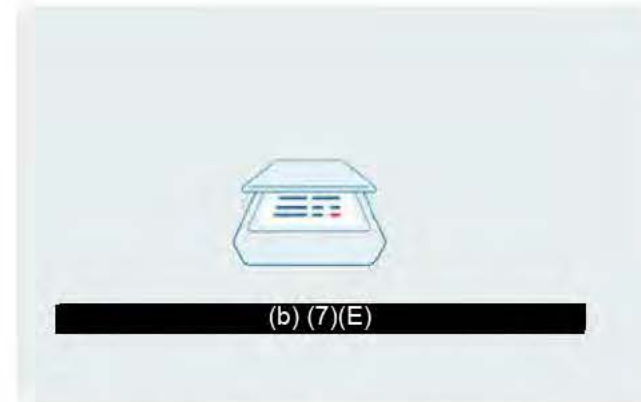


ENROLLMENT

Select a path to begin.



Scanner status is green



Scanner Status is red



Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(6), (b)(7)(C), (b)(7)(E)

Withheld in Full Pursuant to, (b)(5)

OCT 10 2019

MEMORANDUM FOR: Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations

FROM: Colleen M. Manaher
Executive Director
Planning, Program Analysis and Evaluation
Office of Field Operations

SUBJECT: Updated Memorandum of Understanding (MOU) with the Peace
Bridge Public Bridge Authority (PBA)

Planning, Program Analysis and Evaluation (PPAE) has prepared an updated MOU with the PBA on the Pre-Arrival Readiness Assessment (PARE) test.

(b)(7)(E)

The initial camera vendor for PARE was Perceptics.

(b)(7)(E)

(b)(5)

Attachments:

- MOU with the Peace Bridge PBA on PARE

Office of Field Operations
Program Planning, Analysis and Evaluation
September 12, 2019

Action Required: Approval and Forward to EAC

Issue: Updated Memorandum of Understanding (MOU) for Pre-Arrival Readiness Assessment (PARE) 2.0

Executive Summary:

- (b)(7)(E)

Background:

- Through the PARE 2.0 pilot, CBP will deploy facial recognition technology within the in-bound commercial environment at the Peace Bridge, NY port of entry. (b)(7)(E)
(b)(7)(E)
- The initial camera vendor for PARE was Perceptics. (b)(7)(E)
(b)(7)(E)
- (b)(7)(E) (b)(5)
- (b)(5)
- (b)(5)

Recommendation:

- IPA recommends that you forward to EAC Todd Owen for signature a new MOU for PARE 2.0 that contains enhanced privacy protections.

Approved Date: (b)(6);(b)(7)(C) Disapproved Date: _____

Needs Discussion/Date: 10/17/19 Modify/Date: _____

Prepared By: (b)(6);(b)(7)(C) PPAAE, (b)(6);(b)(7)(C)

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DEPARTMENT OF HOMELAND SECURITY,
U.S. CUSTOMS AND BORDER PROTECTION
AND
BUFFALO AND FORT ERIE PUBLIC BRIDGE AUTHORITY
REGARDING THE IMPLEMENTATION OF A PRE-INSPECTION TRAFFIC
MANAGEMENT PROGRAM

The Department of Homeland Security (DHS), through U.S. Customs and Border Protection (CBP), and the Buffalo and Fort Erie Public Bridge Authority (PBA), hereinafter referred to collectively as the “Participants”,

HAVING REGARD for the long-standing cooperative relationship between the PBA and the United States;

RECOGNIZING that the Participants share a common desire to optimize traffic flow across the Peace Bridge, as well as to increase security and decrease processing time at the Port of Entry through the collection of advance information including collection of license plate and commercial truck traveler photo images by the PBA;

COMMITTED to improving commerce and security at the Peace Bridge border crossing, while reducing border crossing wait and processing times;

CONFIRMING that this Memorandum of Understanding (“MOU”) is intended to improve security and efficiency of commercial vehicle processing at the Peace Bridge border crossing,

Hereby express their intent to cooperate as follows:

I. PURPOSE AND SCOPE

The purpose of this MOU is to facilitate the implementation of the PBA’s Pre-Arrival Readiness Evaluation (PARE) program, an automated traffic management system on PBA property in Fort Erie, Ontario, Canada to optimize traffic flow on the Peace Bridge. The objectives of the program are to decrease border congestion and wait times, increase the percentage of commercial drivers who are prepared for processing upon arrival in the United States, and prioritize access to the U.S. CBP Truck Primary inspection lanes for eligible commercial trips. Enhancements to and/or expansion of the PARE program may occur as technological innovations provide

opportunities to implement solutions to further improve traffic management and further mitigate border congestion and wait times.

II. PRIOR ARRANGEMENTS

The MOU signed by the PBA on November 22, 2016 and by CBP on December 2, 2016 is superseded by this MOU upon execution by all signatories.

III. RESPONSIBILITIES

- A. PBA intends to designate a staging area for Commercially Owned Vehicles (COVs) on PBA property in Fort Erie, Ontario, Canada, and direct all COVs through this staging area.
- B. PBA, using its own equipment, intends to capture a photo image of the license plate of each COV and its occupants entering the staging area, and package and transmit over internet/DHS OneNet using encrypted and secure protocol, HTTPS/SSL and HTTPS basic authentication to the CBP PARE middle-tier services hosted in CBP CACE.
- C. PBA shall comply with all applicable DHS/CBP privacy and data protections policies, guidance, and compliance documentation. This documentation includes, but is not limited to, the following: Traveler Verification Service (TVS) business requirements; privacy standards described in DHS/CBP Privacy Impact Assessment for PARE 1.0; DHS/CBP Privacy Impact Assessment for TVS; the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information; and additional applicable DHS/CBP policies or guidance that may be issued during the period of performance of this Agreement.
- D. No photos and/or traveler-related data captured to facilitate CBP's use of TVS may be stored and/or retained by PBA. All photos and traveler-related data must be immediately purged by PBA following transmission to CBP. PBA shall work with CBP to implement a mutually agreeable mechanism by which CBP is able to audit compliance with this requirement.
- E. Upon receipt of the information transmitted by the PBA, CBP intends to use the license plate details to retrieve manifest information to verify whether a manifest has been filed and the border crossing fee has been paid, and intends to transmit a message back to PBA to indicate the status. Also, CBP intends to use the photo image of the COV occupants to verify the identity of the travelers through CBP's TVS matching service.
- F. In the event CBP confirms that a COV has not filed a manifest or paid the border crossing fee, the PBA may notify the COV driver that all documents and fees required by CBP must be filed before the PBA will permit the COV to proceed across the Peace Bridge.

- G. The PBA intends to provide COV drivers electronic access to the internet in the staging area to use to file their eManifest and or pay their user fees.
- H. Each Participant intends to promptly notify the other if at any point it is, or will be, unable to carry out the terms of this MOU (including temporary interruptions in activities).
- I. The collection of photo images of license plates and COV occupants by the PBA, the subsequent sharing of such data with CBP, and any other actions undertaken by PBA in the implementation of this MOU is intended to be conducted strictly pursuant to the PBA's own authority as the owner/operator of the Peace Bridge. CBP personnel are not assigned to Canada as part of this MOU and nothing in this MOU is to be construed as permitting CBP to exercise any authority in Canada or delegating any authority to the PBA to act on its behalf.
- J. CBP intends to retain limited transactional information, consisting only of a date/time stamp of the PBA photo image of the COV license plate and COV occupants, and the source of the transaction (IP address) in CBP system audit logs.
- K. PBA shall ensure that any contractor or subcontractor acting on behalf of PBA in carrying out activities under this MOU fully complies with the applicable terms of this MOU.

IV. GENERAL ADMINISTRATION

- A. The Participants designate the following officials (Designated Officials) for purposes of implementing this MOU:
 - 1. For PBA:**
IT Manager
Buffalo and Fort Erie Public Bridge Authority
 - 2. For DHS/CBP:**
Assistant Port Director
Port of Buffalo, New York
U.S. Customs and Border Protection
- B. Each Participant intends to separately provide, in writing, at the time of signature of this MOU, specific contact information for its Designated Officials to the other Participant and subsequently inform the other promptly in writing of any change to this information to ensure it remains current.
- C. The Participants intend to ensure all requests regarding the administration of this MOU and information provided in response thereto is communicated between their Designated Officials.

V. COSTS

Each Participant is expected to be responsible for its own costs incurred in the implementation of this MOU, except as otherwise mutually agreed in writing by the Participants. All activities under this MOU are subject to the availability of funds and other resources.

VI. APPLICATION AND INTERPRETATION

- A. This MOU is an arrangement between the Participants and does not constitute a legally binding agreement. It is not intended to create, and should not be construed as creating any right or benefit, substantive or procedural, enforceable at law or otherwise.
- B. The Participants intend to modify as necessary, prior to the electronic transmission of any new information under this MOU, the existing Trade Virtual Private Network (TVPN) Interconnection Security Agreement.
- C. The Participants intend to resolve any difference in the interpretation or application of this MOU through consultations.
- D. Each Participant may discontinue cooperation under this MOU at any time with immediate effect, but is expected to provide at least thirty (30) days written notice prior to such termination.

V. APPROVAL

This MOU represents the understanding reached between CBP and PBA. By signing below, the Parties have caused their duly authorized representatives to execute this MOU.

For U.S. Customs and Border Protection

(b)(6);(b)(7)(C)

Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

Date: 10/17/19

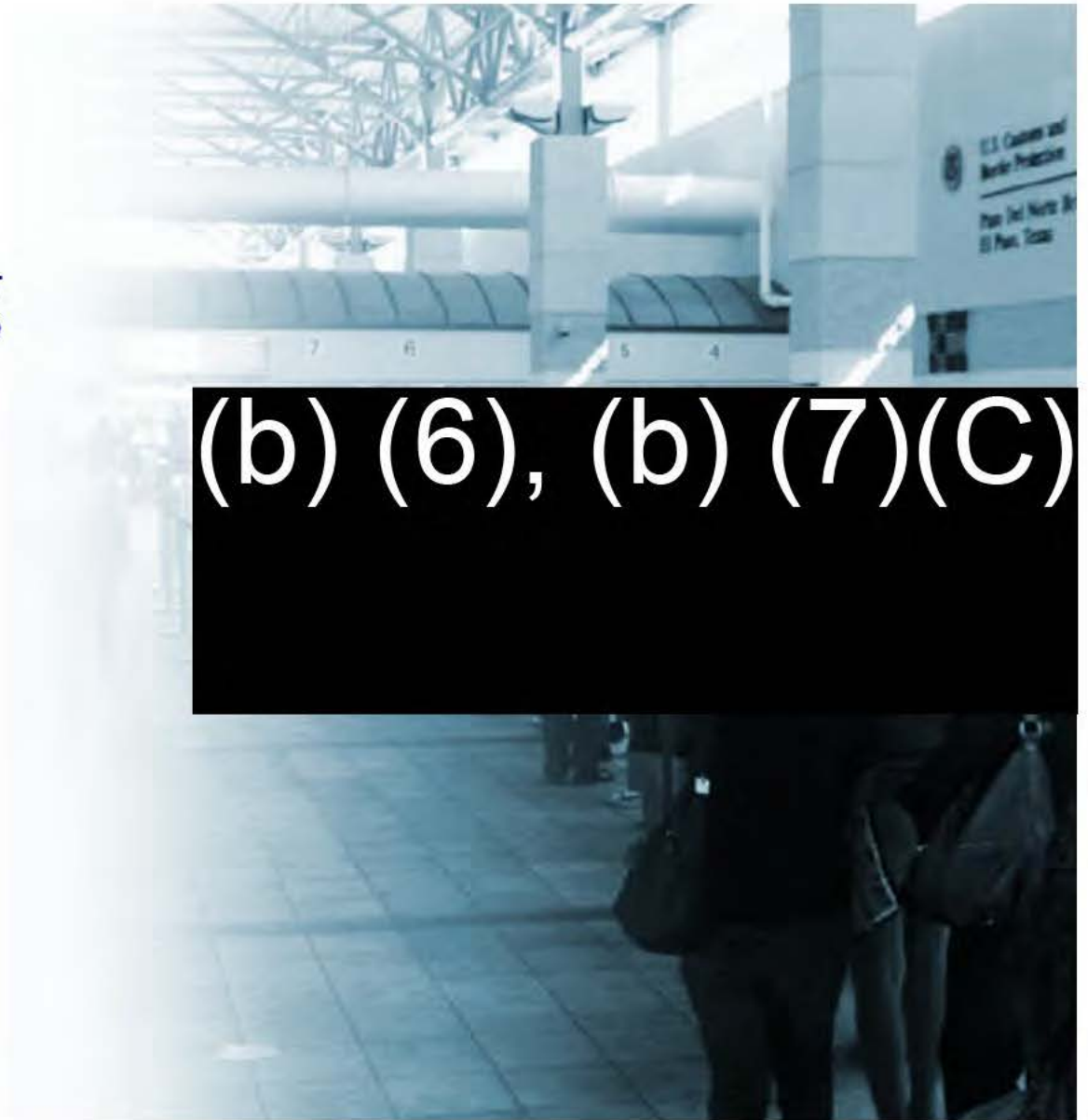
For the Buffalo and Fort Erie Public Bridge Authority

(b)(6);(b)(7)(C)

Buffalo and Fort Erie Public Bridge Authority

Date: 30 SEPTEMBER 2019

Pedestrian Reengineering



Many to Many Processing



U.S. Customs and
Border Protection

Many to Many Processing



**Ready
Lane**

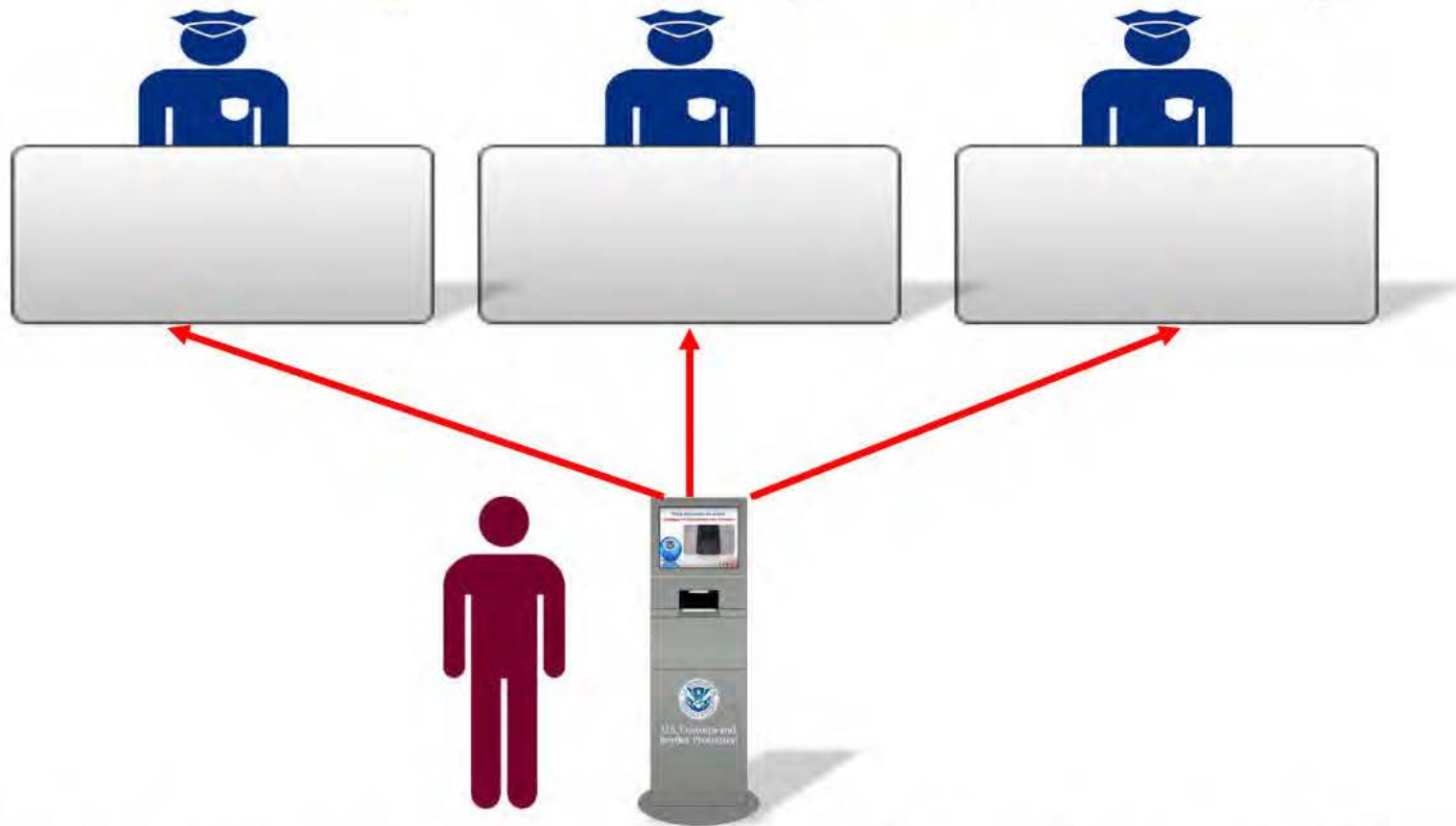


One kiosk serves multiple workstations and conversely multiple kiosks serve one workstation



U.S. Customs and
Border Protection

Many to Many Processing

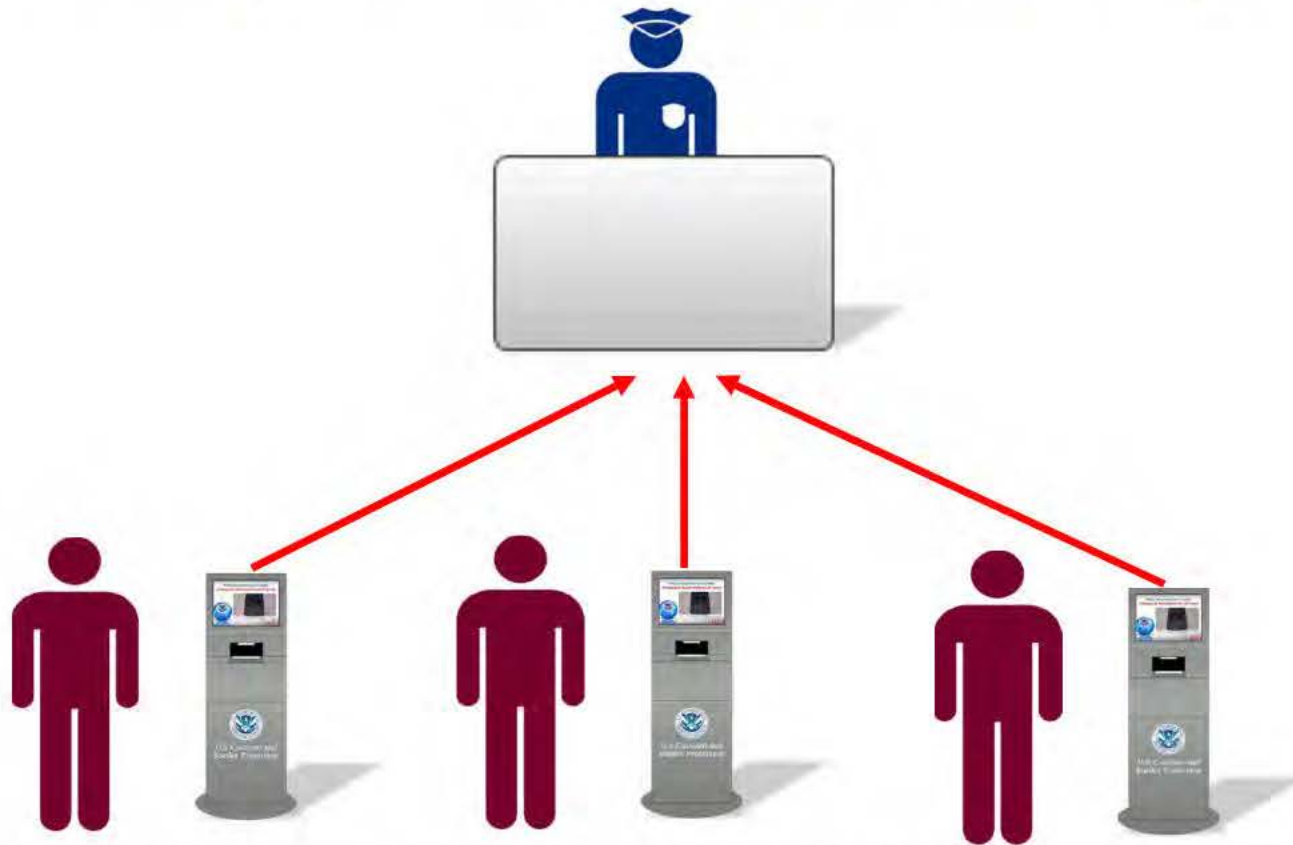


A traveler approaches a kiosk and now may be called by any one of three officers



U.S. Customs and
Border Protection

Many to Many Processing



Multiple travelers approach kiosks, who will be processed, in turn by one officer



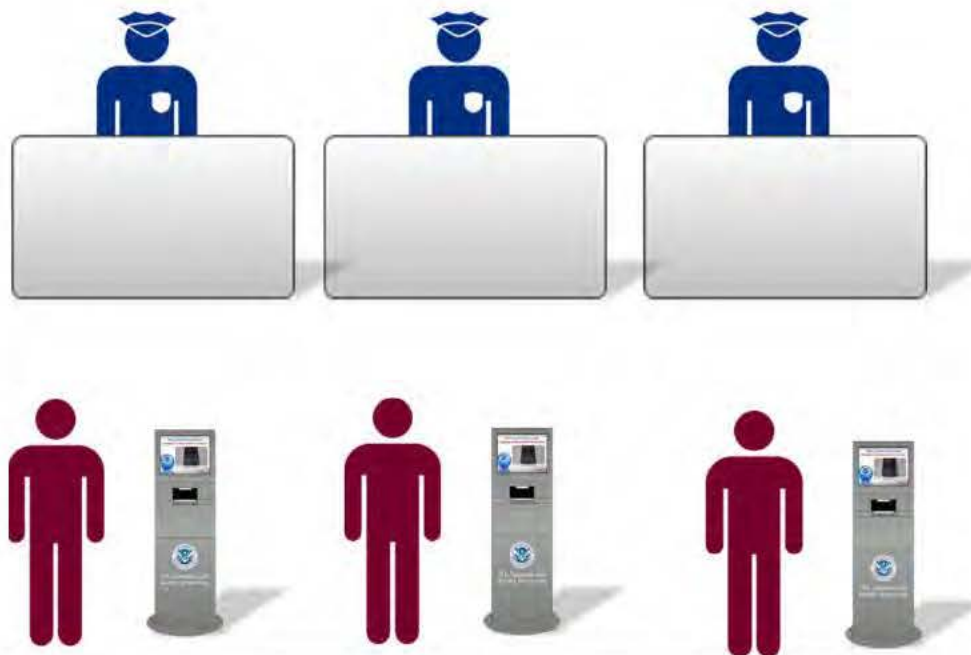
U.S. Customs and
Border Protection

Many to Many Processing



U.S. Customs and
Border Protection

- Ensuring all kiosks remain open improves throughput and enhances officer productivity by reducing the time an officer must wait for a traveler to present documents.
- OFO recommends all kiosks remain open even when the associated workstation is not open.



U.S. Customs and
Border Protection

Many to Many Scenarios

Scenario – Optimal Lane Flow (the traveler in lane 2 is not ready for processing). (b) (7)(E)

(b) (7)(E)

Process – The officer in lane 2 can now call traveler in lane 1 or lane 3 without having to wait for the traveler in lane 2.

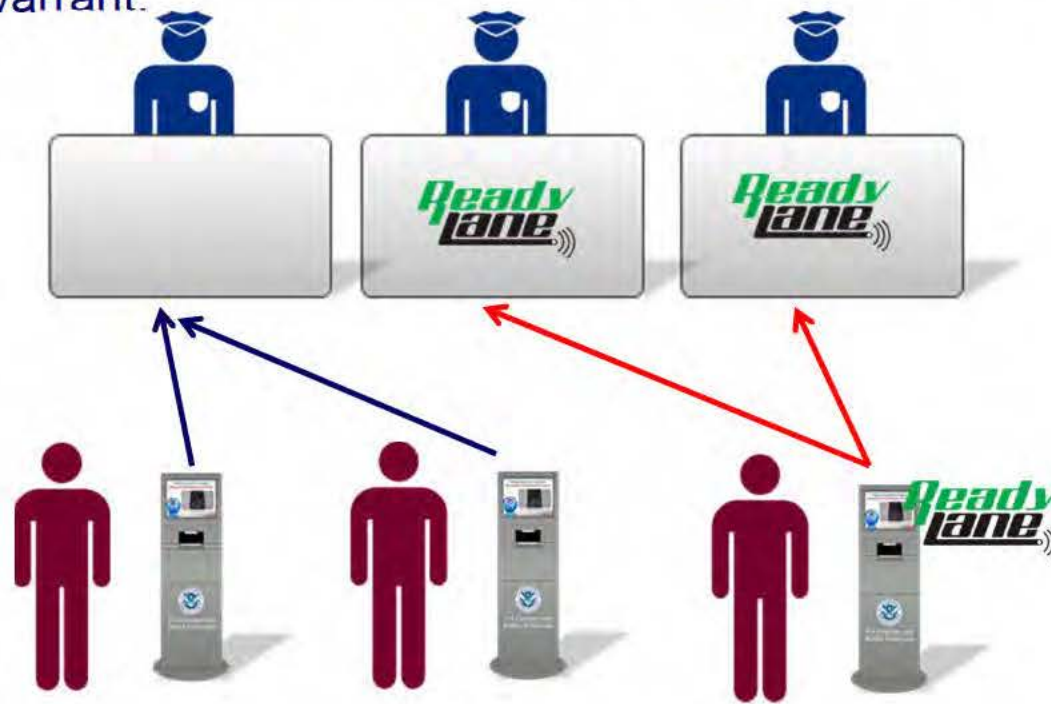


U.S. Customs and
Border Protection

Many to Many Scenarios

Scenario – Active Lane Management

Process – Many to Many processing allows port managers to monitor throughput and designate additional Ready Lanes or general lanes immediately as conditions warrant.

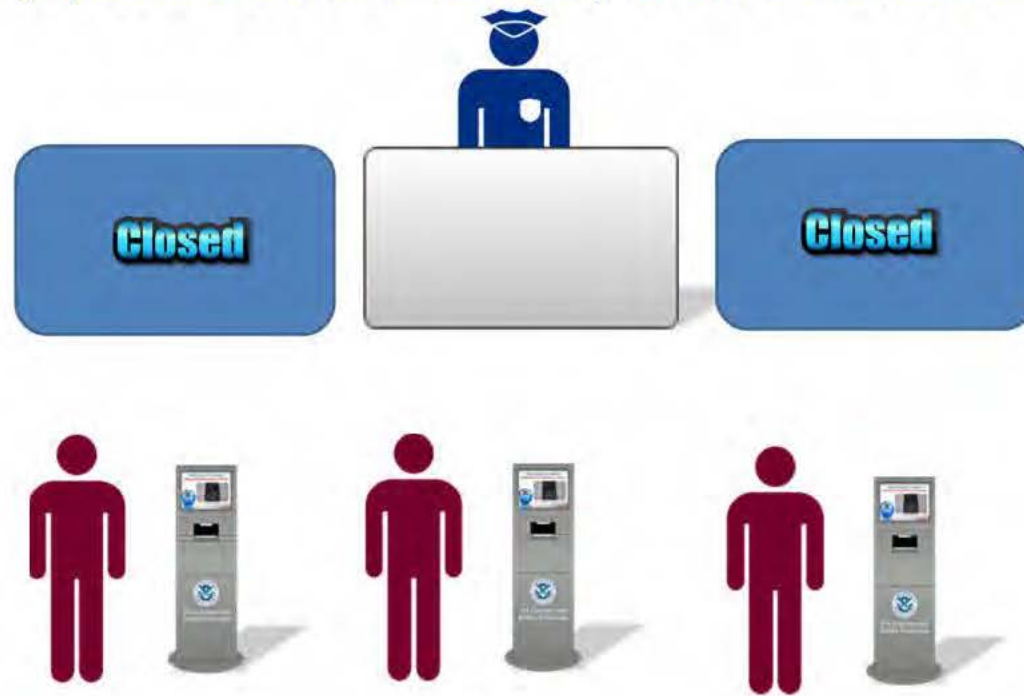


U.S. Customs and Border Protection

Many to Many Scenarios

Scenario – Low Volume Traffic

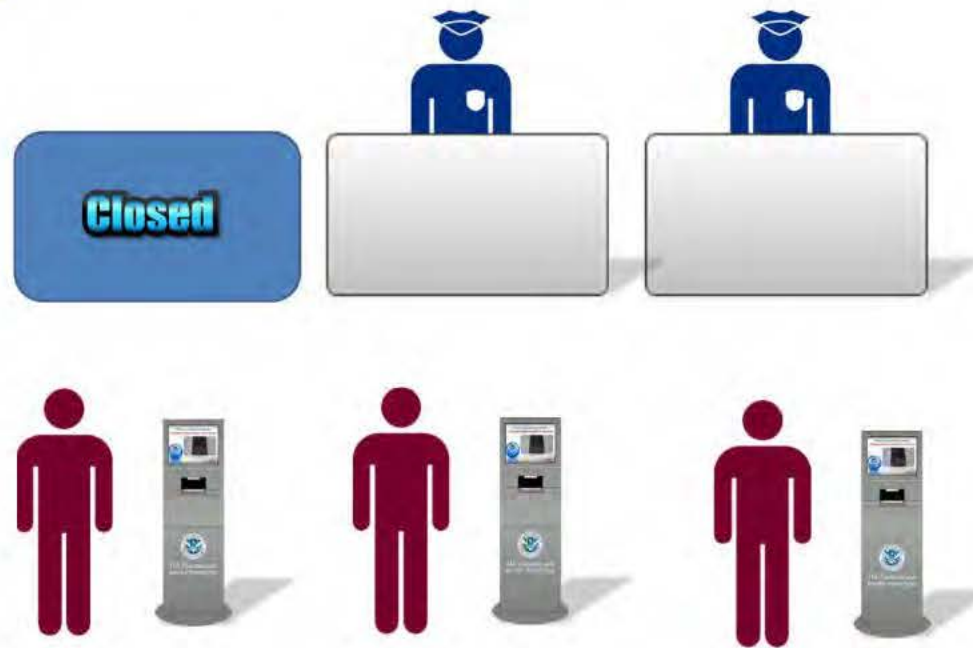
Process – Many to Many processing allows all kiosks to remain open. This improves throughput as travelers are ready when the officer is ready.



U.S. Customs and
Border Protection

Many to Many Scenarios

Scenario – Secondary Escort Required/ Unexpected Lane Closure
Process – Many to Many processing allows the kiosk to remain open until the officer returns.

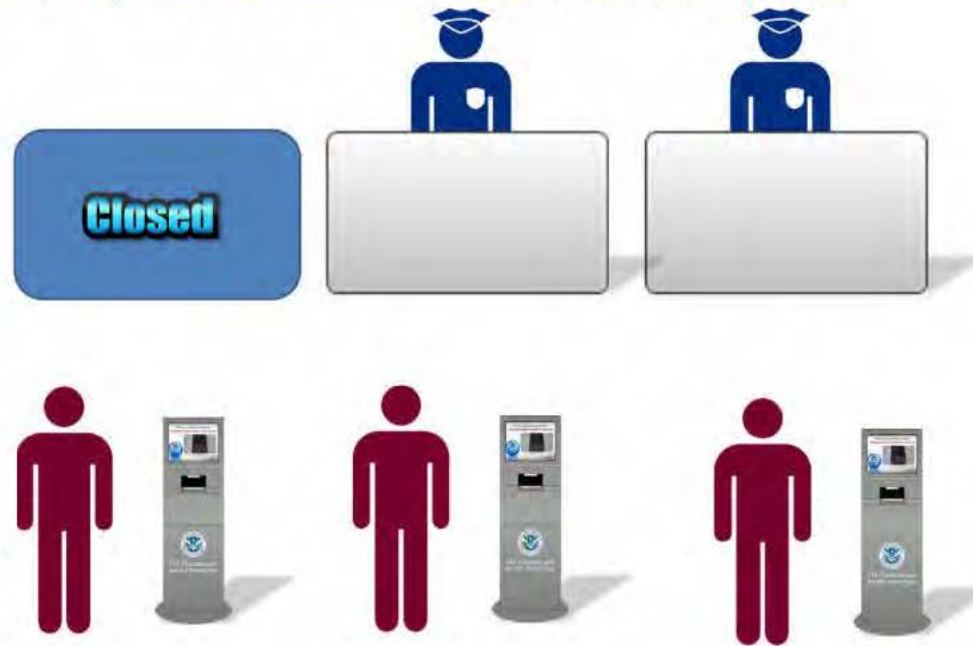


U.S. Customs and
Border Protection

Many to Many Scenarios

Scenario – Shift Changes/Short Term Lane Closure

Process – Many to Many processing allows the kiosk to remain open until the shift change is complete and the workstation re-opens.



U.S. Customs and
Border Protection



U.S. Customs and Border Protection



U.S. Customs and
Border Protection



U. S. Customs and Border Protection
Biometric Air Exit
Business Requirements

Version 2.0
January 2020

Approvals

(b)(6), (b)(7)(C)

2/4/2020
Date

Approved by:

(b)(6), (b)(7)(C)

Acting Executive Director
Planning, Program Analysis and Evaluation
Entry/Exit Transformation
Office of Field Operations
U.S. Customs and Border Protection

Revision Summary

Version	Date	Remarks
1.0	September 19, 2018	Initial draft developed
1.1	November 1, 2018	Updated
1.2	August 1, 2019	Updated
2.0	December 1, 2019	Updated to include additional security requirements.
2.0	January 6, 2020	Inclusion of Appendices
2.0	February 4, 2020	Final edits for approval

This Page Intentional Left Blank

Table of Contents

1. Introduction.....5
 1.1 Background..... 5
 1.2 Purpose 5
2. Definitions.....6
3. Business Requirements6
4. Acknowledgement Declaration 15
Appendix A: Traveler Verification Service Onboarding Guide..... 14
Appendix B: CBP Privacy and Security Principals..... 15

1. Introduction

1.1 Background

U.S. Customs and Border Protection (CBP) is congressionally mandated to implement a biometric entry-exit system.¹ In 2017, CBP developed an integrated approach to a comprehensive biometric entry-exit system that stakeholders, including other U.S. government agencies and travel industry partners such as airlines, airports, and cruise lines, can incorporate into their respective operations. CBP offered relevant stakeholders, also known as business sponsors, an “identity as a service” solution that uses facial comparison technology to automate manual identity verification, and complies with the Congressional mandate for biometric exit. This harmonizes the data collection and privacy standards each stakeholder must follow.

CBP’s Traveler Verification Service (TVS) offers a process for compliance with the pre-departure clearance of passengers under the Intelligence Reform and Terrorism Prevention Act. TVS uses facial comparison technology in a cloud environment to match live traveler photos with photos maintained in U.S. Government holdings. Stakeholder participation in biometric exit is voluntary and is not mandated by CBP. Furthermore, the biometric exit program is designed to facilitate a public – private partnership wherein business sponsors procure and maintain biometric equipment that uses TVS to efficiently and effectively fulfill the biometric exit requirement for in-scope passengers.² Through partnerships with various business sponsors, CBP is enabling a large-scale transformation that will facilitate air travel, while making it more secure, in fulfillment of DHS mission responsibilities.

1.2 Purpose

The purpose of this document is to identify the business requirements for airlines and airport authorities to participate in biometric exit. Additionally, this document provides a list of operational recommendations that should be accounted for when onboarding new sites.

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

² An “in-scope” traveler is any person who is required by law to provide biometrics upon exit from the United States pursuant to 8 CFR 235.1(f)(ii). In-scope travelers include any aliens other than those specifically exempt as outlined in the CFR.

2. Definitions

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

3. Business Requirements

This section describes the business requirements for Biometric Air Exit. The term ‘system’ in Section 3 refers to any physical equipment, software and/or any resource involved in the Biometric Air Exit process.

#	Requirement	Comments
1	The business sponsor and its systems integrator must adhere to the requirements outlined in this document and the technical on-boarding guide attached as Appendix A.	A business sponsor must be an airline and/or airport authority that facilitates the use of TVS to implement biometric exit. In addition to Appendix A, the CBP TVS New User Access Request (UAR) Form and TVS-In-A-Box New UAR Form are available upon request.

#	Requirement	Comments
2	The business sponsor must return a signed copy of this document's acknowledgement and compliance page, which confirms receipt of the program's business requirements and records the business sponsor's agreement to comply with the requirements.	Any TVS-related contract between a business sponsor and another organization (e.g., a systems integrator, vendor, or other third party) must detail the specified actions and measures that will be taken to ensure compliance with all relevant business requirements contained herein and Technical Reference Guides (TRG).
3	The business sponsor and its systems integrator must submit and receive approval for a proposal, which incorporates the use of TVS. For approval, the business sponsor is required to submit information including: network topology, high-level solution architecture, test schedule, and deployment plan. In addition, the business sponsor must provide CBP with the camera's manufacturer information, including name, model, serial number, and firmware version.	<p>The TVS TRG contains specific requirements. Any required infrastructure and equipment must be procured and maintained by the business sponsor and/or its vendor. Upon the release of an updated version of the TRG, the business sponsor must provide a plan and a reasonable timetable to bring the solution back into compliance with any Government-mandated changes. Any changes that are identified as "mandatory" must to be implemented as soon as technically possible, but no later than 60 days. CBP may provide an extension upon request.</p> <p>Upon review of the aforementioned documents (e.g., solution architecture), CBP may request additional IT and security documents from the business sponsor. Examples may include but are not limited to: the DHS Security Requirements Traceability Matrix (RTM); and/or FEDRAMP certification. All CBP requests for security documentation must be fulfilled and approved prior to "Go-Live" and connectivity with CBP's Production environment. Existing partnerships will be required to comply within an agreed upon timeframe.</p>

#	Requirement	Comments
4	The business sponsor and its systems integrator must adhere to the CBP prescribed naming convention for device unique identifiers (i.e., camera's "Device_ID"). The scheme should comply with the following: (1) Port; (2) Terminal; (3) Gate; (4) Camera Model; and (5) Camera number. An example Device_ID is ATL-E-014-Vendor-01.	The TVS TRG mandates compliance with the Device_ID scheme on message elements. If the vendor recommends a different approach, CBP will consider all requests.
5	The business sponsor must provide the required power for use of TVS, as well as reliable and secure network access (e.g., high-speed internet and/or cellular).	The TVS TRG contains specific internet requirements. Cellular networks are also required to support CBP Officer mobile devices that will be used to perform exception processing of travelers.
6	The business sponsor and all relevant third parties (e.g., airlines and port authorities) must comply with applicable DHS/CBP security and privacy policies and compliance documentation. Business sponsors and participating organizations should ensure their own privacy policies and notices are updated. CBP will conduct compliance reviews on a periodic basis.	The business sponsor must provide CBP with the site's network/internet bandwidth no later than the activation of the solution. The TVS Privacy Impact Assessment (PIA) contains a complete list of applicable privacy policies (e.g., posting DHS-branded signs in close proximity of and prior to the cameras, provide CBP-approved tear sheets, boarding gate announcements, and facilitation of exemption processing for travelers who elect to opt-out). If e-signage is used, the CBP-approved language must be visible for the entirety of the boarding process.
		The current TVS PIA, along with the applicable appendices and its predecessor PIAs, can be found at: www.dhs.gov/privacy

#	Requirement	Comments
7	Any photos taken to facilitate TVS matching must not be stored and/or retained by the business sponsor or its systems integrator/vendor. All photos must be immediately purged from the business sponsor's system upon the photo's transmission to TVS. The business sponsor's system (including its systems integrator) must provide a mutually agreeable method by which CBP is able to audit compliance with this requirement.	<p>CBP will consider requests by the business sponsor to retain the Advance Passenger Information System (APIS) Unique Identification Number (UID) and matching result (assuming compliance with DHS/CBP privacy requirements).</p> <p>An approved partner may collect photos of travelers using its own equipment under its own separate business process for its own commercial purposes. In this scenario, the business sponsor must distinguish its process from CBP's TVS enabled one through signage and other forms of public notice.</p>
8	Any public communications regarding TVS performance or CBP's biometric exit program must be coordinated with CBP prior to release to the public or media. Any marketing campaigns and multimedia content related to CBP, TVS, or the biometric exit program must be approved in advance and in writing by CBP.	<p>Public releases that do not reference CBP or any of its programs and systems (such as TVS) do not require CBP coordination or approval.</p> <p>Public releases that do reference CBP or any of its programs and systems should be coordinated as soon as possible. CBP recommends at least 7 days in advance to ensure prompt approval.</p>
9	To provide a consistent passenger experience, all TVS-enabled equipment throughout the traveler continuum must apply a set of consistent traveler-facing indicators. The following indicators must be used and visible to both travelers and airline/CBP staff:	<p>CBP will consider requests by the business sponsor to alter the defined list of indicators.</p> <p>The messaging for the blue light indicator can vary by vendor and/or stakeholder. An example of messaging: "Please see gate agent."</p>

Color	Symbol	Meaning
Blue	X	No Match
Yellow	Refresh	Recapture or Error/Issue
Green	Checkmark	Match/Board

#	Requirement	Comments
10	Any system log files and data stored, associated with a TVS-enabled biometric exit solution transaction data, must be approved by CBP to ensure compliance with DHS and CBP privacy and security policy.	The log files and data may be subject to select privacy and security policies depending on their content, retention period, and purpose. All data must be encrypted at rest and in transit.
11	For TVS performance standards, the TVS TRG contains requirements for system scalability, availability, and maintainability.	The TVS TRG states “Reliable, high-speed internet access is required. A hard-wired connection is preferred, but high speed wireless will be adequate if the connection can be made reliable.”
12	CBP must be allowed to review and/or audit any code, encryptions, network connections and any other TVS related technical specifications.	
13	The business sponsor must ensure that CBP-approved signage is posted at each gate location, while the biometric boarding processing is ongoing. This is described below. The signage must be clearly visible and placed at a sufficient distance in front of the camera in order to provide the traveler with a reasonable opportunity to read the content and opt-out before reaching the photo capture area.	Any updates to CBP mandated privacy signage must be posted as soon as possible (e.g., sufficient time for fabrication and posting). Business sponsors can find the most current version of communication materials on the CBP website. www.cbp.gov/biometrics

Where signage is at least 22 inches wide and 28 inches tall, only one sign needs to be present. If signage is smaller than 22 inches wide and 28 inches tall, a minimum of two signs need to be present unless accompanied by e-signage (described below). Posted signage should never be smaller than 7 inches wide and 11 inches tall.

Business sponsors can elect to display e-signage in either a static or slide show format. Should e-signage be displayed as part of a slide show, it must be visible for at least 45 seconds once every 5 minutes and be accompanied by at least one posted sign of a size no smaller than 7 inches wide by 11 inches tall. If the signage is displayed in a static format, it must be maintained as such throughout the entirety of the boarding process.

#	Requirement	Comments
14	CBP will distribute TVS performance data to the business sponsor (and relevant biometric exit program stakeholders) on an agreed-upon frequency that is operationally sustainable.	
15	CBP may request ad hoc performance reporting on select systems integrated with TVS. Examples include, but are not limited to: (a) estimated number of opt-outs; (b) camera capture rates; (c) number of travelers processed; (d) average photo quality scores; and (e) percentage of photos taken that were below the prescribed quality threshold.	
16	Upon the identification of a system performance issue, the business sponsor and its systems integrator must provide a detailed remediation plan and schedule. The business sponsor will provide progress reports to the CBP Biometric Exit Program Office on a mutually agreed-upon interval.	All remediation schedules must be completed as quickly as possible.
17	CBP must be notified of any cybersecurity-related incidents or breaches that occur on networks and hardware maintained by airport authorities and airlines which are integrated with CBP's TVS. All known or suspected incidents or breaches shall be promptly reported to the CBP Biometric Exit Program Office, CBP Privacy Office, and CBP Security Operations Center within 24 hours after discovery of a suspected incident or within 1 hour after a suspected incident has been confirmed, whichever is earlier.	<p>This requirement begins immediately once TVS integration is operational.</p> <p>Points of Contact:</p> <ul style="list-style-type: none">• Biometric Exit Program Office: [REDACTED] (b)(7)(E)• CBP Privacy Office: [REDACTED] (b)(7)(E)• CBP Security Operations Center: [REDACTED] (b)(7)(E) <p>Source: DHS Privacy Incident Handling Guidance (https://www.dhs.gov/publication/privacy-incident-handling-guidance-0)</p>

#	Requirement	Comments
18	The sponsor and/or vendor must ensure that all access to the hardware is secured and restricted to authorized personnel only. CBP does not permit any unsecured methods of externally accessing the camera (e.g., interfaces or ports such as USB). Furthermore, access to the system and its endpoints must require no less than a username/log-in and password.	
19	The business sponsor's system must be designed to include a time-out mechanism for each camera when not in use for boarding operations.	The "time-out" feature should minimize any unintentional photographs taken of travelers that are not attempting to board the plane.
20	Business sponsors are responsible for ensuring their participation in any TVS-related program is done in compliance with applicable federal and state laws and their relevant contracts. This includes any decision to integrate an e-gate into the biometric exit solution. The business sponsor must confirm such equipment is compliant with applicable codes that govern relevant operations within your jurisdiction (e.g., fire code, the Americans with Disabilities Act, etc.).	
21	All maintenance of the equipment and software development provided by the business sponsor or relevant stakeholder in support of the TVS-related program is the responsibility of that business sponsor and/or the relevant participating stakeholders. Any personnel with access to equipment that is located airside must meet airport security requirements for access to secured areas. Airport security screening requirements may include criminal history, background, and fingerprint check and CBP vetting.	

#	Requirement	Comments
22	The business sponsor and its systems integrator may not use any equipment to collect and send data to TVS, which has been manufactured by, or has parts that have been manufactured by, any company that is banned by statute or regulation from being purchased by a Federal Government agency, or is suspended or debarred for federal contracts. This includes Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 and the System for Award Management (SAM).	This covers video surveillance and telecommunications equipment produced by ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities), whom the Federal Government is banned from using for national security reasons.
23	All relevant business sponsor and system integrator personnel are required to review CBP's Privacy and Security Principles.	Please see Appendix B for a list of CBP's Privacy and Security Principles.

4. Operational Considerations and Recommendations

This section describes the operational considerations for carriers conducting biometric exit.

#	Operational/Onboarding Considerations	Comments
1	The business sponsor and its systems integrator must submit and receive approval for its deployment schedule.	
2	In the event that a traveler does not match through TVS, the airline personnel (or its designee) at the boarding gate should verify the traveler's identity against his/her travel document before permitting the traveler to board the aircraft. If there is any concern about the authenticity of the travel document, or any concerns that the traveler is not the true bearer of the document, CBP can be contacted to adjudicate the matter. CBP will respond as soon as operationally possible. Operating under its own authorities and business processes, the airline can choose not to board the traveler if the traveler's identity is not adjudicated by CBP in time to allow for a timely departure.	The business sponsor and all relevant airlines must ensure that all boarding gate personnel operating international departure boarding gates are trained on alternative manual processing for persons who do not match through TVS.
3.	It is highly recommended that all carriers provide boarding announcements prior to boarding and periodically throughout the boarding process. The boarding gate announcements should clearly convey the use of TVS for purposes of boarding	Please see www.cbp.gov/biometrics for the most current version of the Biometric Boarding Gate Announcement script and/or recording that gate agents should use.

	and disclose the ability of travelers to opt-out of the process.	
4	If the business sponsor is an airline then the airline must ensure all flight schedules, diversions, delays and departure times are updated within the relevant systems as soon as possible.	TVS is designed to ensure galleries are staged and removed "just in time." Therefore, if a flight is significantly delayed without a corresponding update with a new departure time, biometric exit processing/boarding may not be available.
5	If the business sponsor is an airline, then the airline must ensure that all identified APIS errors are corrected prior to departure to facilitate comprehensive gallery creation.	Gallery creation is dependent on accurate API data. If API is incomplete, it must be updated during check-in or prior to boarding. TVS updates the photo galleries every 5 minutes, beginning 2 hours prior to departure.

Acknowledgement and Compliance Declaration

I, (b)(6), acknowledge that I have received and read the Biometric Exit Business Requirements Document (BRD) and Technical Reference Guide (TRG) on behalf of the Port of Seattle, and agree to comply with the contents as of the date of signature.

Signature:

(b)(6)

Name:

Title:

Date:

3/13/20

Appendix A: TVS Onboarding Guide

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

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

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

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

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

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

Please send all completed forms to the CBP TVS Team using the email (b)(7)(E)

Appendix B: CBP Privacy and Security Principles

FAIR INFORMATION PRACTICE PRINCIPLES (DHS FIPPs)

- **Transparency**: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation**: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- **Purpose Specification**: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization**: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation**: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security**: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.³

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



Homeland Security

DEC 09 2019

MEMORANDUM FOR: Mark Borkowski
Component Acquisition Executive
U.S. Customs and Border Protection

FROM: (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)
Acting Chief Financial Officer

SUBJECT: U.S. Customs and Border Protection Biometric Entry-Exit Life Cycle Cost Estimate

In accordance with my duties and responsibilities, I approve the U.S. Customs and Border Protection (CBP) Biometric Entry-Exit (BEE) Life Cycle Cost Estimate (LCCE) dated October 16, 2019.

The Department of Homeland Security (DHS) Cost Analysis Division (CAD) reviewed the CBP BEE LCCE dated October 16, 2019 and also conducted an Independent Cost Assessment (ICA) to validate the estimate's results. The ICA analyzed the most critical cost elements and concluded that the BEE LCCE is an accurate and credible cost estimate. CAD identified the following recommendations for the CBP Biometric Entry Exit to address in the next LCCE:

- CBP Biometric Entry-Exit PMO should continue to monitor, update, and document actual costs for future LCCE updates and provide DHS CAD with annual updates no later than April 1 of each calendar year until all segments are post full operating capability (FOC).
- For future CBP Biometric Entry-Exit LCCE, Land and Sea Segments, the Program Management Office (PMO) cost team should:
 - (b)(5)
 - (b)(5)
 - (b)(5)
 - (b)(5)
- Add risk and uncertainty analysis at the input level of the cost model for more precision (lower level WBS elements for build-up).

The CBP BEE LCCE, as pictured in Attachment 1, totals \$1,831M Then Year (TY) at the 50% Confidence Level. This approved LCCE shall be used to inform the upcoming Acquisition Program Baseline update and future budget requests.

I request the Customs and Border Protection Biometric Entry-Exit Program Office update the Program LCCE on an annual basis.

Should you have any questions, please contact (b)(6), (b)(7)(C), CAD, at (b)(6), (b)(7)(C), (b)(6), (b)(7)(C).

cc:

Colleen Manaher, Program Manager

(b)(6), (b)(7)(C), Director, CBP OA Acquisition and Policy Oversight

(b)(6), (b)(7)(C), Executive Director, Office of Program Accountability and Risk Management

(b)(6), (b)(7)(C), Director, OCFO Program Analysis & Evaluation

(b)(6), (b)(7)(C), Director, OCFO CAD

Attachment(s)

1. CBP BEE Risk Adjusted Results for LCCE dated [11.14.2019]
2. CBP BEE ICA Report [12.04.2019]
3. CBP BEE Certification of Funds Memo [11.09.2019]



Department of Homeland Security
Customs and Border Protection (CBP)

Biometric Entry-Exit Life Cycle Cost Estimate Documentation

Version 2.0

Submitted by:	(b)(6), (b)(7)(C) Program Manager	October 9, 2019 10/16/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Program Acquisition Executive	10/19/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Lead Business Authority	10/16/19 Date
Endorsed by:	(b)(6), (b)(7)(C) Component Chief Financial Officer	8 Nov 19 Date
Endorsed by:	(b)(6), (b)(7)(C) Component Acquisition Executive	9 Nov 19 Date
Endorsed by:	(b)(6), (b)(7)(C) DHS Cost Analysis Division	12/6/19 Date
Approved by:	(b)(6), (b)(7)(C) DHS Chief Financial Officer	12/9/19 Date