Capability Analysis Report for Biometric Entry-Exit

Sponsoring Organization: U.S. Customs and Border Protection, Office of Field Operations

Sponsoring Organization Primary Point of Contact: (b)(6) (b)(7)(c)
PPAE, Executive Director, (b)(6) (b)(7)(c)

Sponsoring Organization Secondary Point of Contact: (b)(6) (b)(7)(c)
PPAE Deputy Executive Director, (b)(6) (b)(7)(c)

March 20, 2017

Validation Page

Submitted: (b)(6) (b)(7)(c) [redacted]

Executive Director / Program Manager Date
Planning, Program Analysis and Evaluation
CBP, Office of Field Operations

Endorsed by: (b)(6) (b)(7)(c) [redacted]

Director Date
Capability & Requirements Division
Planning, Analysis, Requirements, and Evaluation Directorate
Operations Support

Validated by: (b)(6) (b)(7)(c) [redacted]

DHS Joint Requirements Council (JRC) Date

Endorsed by: (b)(6) (b)(7)(c) [redacted]

DHS Joint Requirements Council (JRC) Date

Table of Contents

Executive Summary

The primary mission for U.S. Customs and Border Protection (CBP) is to safeguard America's borders from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling lawful international trade and travel. CBP is required by law and executive order to implement measures for verification of identities for all travelers, including United States (U.S.) citizens, upon entry to and exit from the U.S. by fusing biographic and biometric data. 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 resident card, or other authorized travel document. Biometric data includes information captured from fingerprints, facial images, or other individual characteristics. Biographic data, when used with biometric data, allows CBP to confirm a traveler's identity with greater assurance, match to previous encounters with CBP, and conduct biometric watch list checks. As biometric technology has evolved, the ability to use individual characteristics to confirm identity for all travelers, including U.S. citizens, is now a reality for all travel modes—air, land, sea.

Currently, CBP collects fingerprints and facial images from most foreign visitors entering the U.S. and uses the biometric database operated by the DHS Office of Biometric Identity Management (OBIM) to confirm identity. However, this biometric matching capability is not available to verify identity of all travelers upon departure from the U.S. CBP and OBIM are currently working together to identify requirements and a timeline when this capability would be available. In parallel, CBP is working to identify matching capabilities that could be utilized while OBIM is developing its biometric identity services.

To understand the breadth of the required capability needs to meet its mission requirements, CBP has prepared this Capability Analysis Report (CAR) to document existing and future capabilities that are required to verify the identities of all travelers. Capability needs and current gaps documented in the CAR were identified through coordination and information sharing on biometric activities with other DHS components, such as Transportation Security Administration (TSA), Science & Technology (S&T) and OBIM. CBP has also conducted a number of small-scale trials of biometric technologies at air and land ports to field test the integration of biometric technologies in entry and exit operations. From these activities, CBP has identified the following capabilities needed to support CBP's border security mission:

- **Verify Traveler Identity** – The ability to capture, review, analyze, search, and match a traveler's biometric information to their biometric and biographic records when entering and exiting the U.S. for the purposes of verifying their identity.
- **Create and Manage Biometric Records** – The ability to capture, store, and disseminate biometric information and metadata collected from travelers entering and, where required, exiting the U.S.
- **Generate Metrics and Reports** – The ability to measure and report the effectiveness of the biometric entry-exit system.

The capabilities defined are driven by mission needs that will also require upgrades, modifications or enhancements to process, technology and physical infrastructure elements

across the CBP operational environment. These needed capabilities will require the existence of a mature communication network infrastructure to connect the inspection areas at CBP ports of entry (POE) to multiple law enforcement and biometric databases; a robust law enforcement information sharing environment required to access, request, search, discover, and retrieve biometric data; and, a safe, secure area for holding, detaining, and processing travelers of interest without impeding normal operations. Additionally, it will require an adequate number of CBP Officers that are fully trained in biometric processes and successfully leveraging traveler behaviors and expectations that do not require new or unexpected steps to maximize efficiencies and minimize wait times.

As potential solutions are identified to enhance or develop these required capabilities, CBP will assess the suitability, feasibility, and achievability against the following operational issues/considerations:

- Does the solution avoid stove-piped, independent approaches?
- Does the solution use existing physical facilities and infrastructure?
- Does the solution support existing business models and processes?
- Does the solution mirror/emulate/support current behaviors to minimize new or unexpected steps for travelers?
- Does the solution use existing data and IT infrastructure?

As a next step, CBP will develop a Mission Needs Statement (MNS), which will further detail CBP mission needs that will be addressed through a biometric entry-exit program and will include linkages to the capability gaps identified in this CAR.

1 CAR Scope

This CAR describes CBP's capabilities with respect to long-term CBP biometric information capture, validation, and enforcement operations at U.S. air, land, and sea POEs for travelers entering and exiting the U.S. Since the transition of the biometric exit portion of the US-VISIT program to CBP in 2013, CBP has developed a strategy that will apply state-of-the-art biometric technology supported by enhanced processes to improve traveler identification and verification. The strategy includes assessing new biometric technologies using operational field trials at POEs while continuously enhancing or replacing current systems, upgrading infrastructure, and transforming operations.

2 Operational Context

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. Every day CBP processes over 1 million travelers as they enter the U.S. at air, land, and sea POEs. By comparison, over 1 million travelers also depart the U.S. daily with approximately 700,000 departing at a land border, 300,000 by an airplane, and 50,000 by a sea vessel. CBP operations in the exit environment is limited to identifying and detaining individuals subject to a law enforcement action or through random inspection of people as they board an airplane or cross a land border.

Under existing laws and Executive Order 13780[1], CBP is required to implement measures that will enable CBP to verify the identities of all travelers, including U.S. citizens. In response, CBP has developed a biometric entry-exit strategy to define, develop, and deliver the necessary capabilities required to verify all traveler identities. This capability will also permit identification of individuals who have violated their terms of admission or who are subject to law enforcement action. CBP intends to establish a comprehensive biometric entry-exit program to enhance the integrity of the immigration system by assuring traveler identity on departure matches to the traveler identity at arrival. With the implementation of biometric checking at departure the daily CBP processing workload will essentially double.

Under this biometric entry-exit program, CBP, in cooperation with DHS components, other relevant Federal agencies, and the private sector, will develop and deploy a comprehensive biometric entry and exit capability in which all travelers requiring the collection of biometric information upon entry to the U.S. will have biometrics collected on exit to validate their identity. This will be applicable at all air, land, and sea ports of entry. DHS has committed to Congress that initial deployments will begin at select U.S. airports in FY 2018.

CBP has prioritized the entry-exit capability development by travel mode—air, land, and sea. This approach allows CBP to effectively plan and schedule so that CBP can address future needs in a logical manner. CBP's top priority for deployment of biometric entry-exit capabilities is in

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

the air environment, followed by land and sea. Each travel mode offers unique challenges that will require integrated solutions to mitigate any potential negative impacts to travel and trade. For example, in the air environment the solution must not impede the normal travel process and must facilitate the flow of travelers boarding the aircraft and be integrated with the airline process. Biometric solutions must be thoroughly designed and tested to ensure that they are effective; compatible with expediting travel; integrated into existing infrastructure, systems, and processes; and, not cost prohibitive.

3 Necessary Capabilities

The CBP mission to inspect and confirm the identity of all incoming and departing travelers requires a suite of enhanced and new capabilities. For travelers seeking entry to and exit from the U.S., CBP requires the capability to discern individuals who are lawfully present in the U.S. from those who have violated their terms of admission. The ability to discern individuals and determine their legal ability to enter and exit the U.S. requires multiple materiel and non-materiel capabilities at all U.S. POEs. Central to the CBP strategy to perform this mission task is the collection and application of biometric data.

To successfully verify traveler identity, one or more biometric modalities will be used to verify identity. A biometric is a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. The most common biometrics in use today include fingerprints, facial image, and iris.

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

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

These mission needs will enable CBP to develop the following required capabilities:

- **Verify Traveler Identity** – The ability to capture, review, analyze, search, and match a traveler's biometric information to their biometric and biographic records when entering and exiting the U.S. for the purposes of verifying their identity.
- **Create and Manage Biometric Records** – The ability to capture, store, and disseminate biometric information and metadata collected from travelers entering and exiting the U.S.

- **Generate Metrics and Reports** – The ability to measure and report the effectiveness of the biometric entry-exit system.

4 Strategic Guidance and Authorities

4.1 CBP Mission Alignment

CBP has the ongoing mission to inspect all incoming and departing travelers and conveyances to determine admissibility to the U.S. 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 U.S. 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.

Table 1, Alignment to CBP Mission Areas, summarizes the five areas of mission needs for biometric entry/exit and aligns them to CBP mission areas outlined in the *CBP Vision and Strategy 2020*[2]. This assessment is based on current CBP operations and findings from biometric field trials.

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

Table 1—Alignment to CBP Mission Areas

4.2 Alignment with DHS Missions

Across DHS, component offices have the need to collect, identify, verify and record subjects encountered during the various enforcement, security, and immigration missions in a manner that fully safeguards and supports secure cyberspace. CBP has been actively examining joint requirements for biometric capabilities across DHS since the inception of the Joint Requirements Council (JRC) and has led several initiatives to improve cross-component collaboration. Along with other DHS components, CBP helped to develop a DHS-wide *Biometrics Strategic Framework*[3] in 2015 and in 2016 the *Biometrics Roadmap Winter Study*[4] to

[2] https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf
[3] https://www.hsdl.org/?view&did=786880
[4] http://dhsconnect.dhs.gov/org/comp/plcy/spar/Winter%20Studies/Biometrics%20Roadmap%20Winter%20Study_Final%20Report_April%2015%202016.pdf

guide biometric implementations across the department. As stated in Section 4.1, CBP performed a number of biometric field trials which identified a series of mission needs that have been aligned to DHS mission areas. Table 2, Alignment to DHS Mission Areas, summarizes the Biometric Entry/Exit mission need alignment to DHS mission areas as identified in the *2014 Quadrennial Homeland Security Review*[5].

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

Table 2—Alignment to DHS Mission Areas

4.3 Authorities

Legal authorities for CBP to collect and utilize biographic and biometric data to confirm identity at the time of arrival to and departure from the United States include:

- Immigration and Nationality Act (INA) § 235 [8 USC 1225], § 287 [8 USC 1357] and § 215 [8 USC 1185]
- 8 CFR § 215.8 Requirements for biometric identifiers from aliens on departure from the United States
- 8 CFR § 235.1 Scope of examination
  - 8 CFR § 235.1(b) Requirement for US citizen to possess valid U.S. passport for entry to or departure from the U.S. (*see also 8 CFR 1185(b)*)
  - 8 CFR § 235.1(f) Alien applicants for admission
- 8 USC § 1187(i) Visa Waiver Program; Establishment of exit system
- 8 USC § 1365b(d)-(h) Biometric entry and exit data system; Collection of biometric exit data; Integration and interoperability; Maintaining accuracy and integrity of entry and exit data system; Integrated biometric entry-exit screening system; Entry-exit system goals
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 7208 and 7209, as amended (P.L. 108-458)
- The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, P.L. 107-56, Sec 414(b))
- Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6)
- Department of Homeland Security Appropriations Act, 2015 (P.L. 114-4)
- Consolidated Appropriations Act, 2016 (P.L. 114-113)
- January 2004 Interim Final Rule (69 FR 468) on Non-Immigrant Visa Travelers

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

- Exit pilots were established in this rule, and updated later in 2004 in 69 FR 46556 and 69 FR 51695.
- August 2004 Interim Final Rule (69 FR 53318) on VWP Travelers and 50 Largest Land Ports
- 50 Largest Land POEs identified in November 2004 (69 FR 64964)
- Remaining Land POEs identified in September 2005 (70 FR 54398)
- December 2008 Final Rule (73 FR 77473) on Additional Alien Categories
- June 2009 Notice (74 FR 26721) on Biometric Air Exit Pilot at Two Airports
- July 2015 Notice (80 FR 44983) BE-Mobile at top 10 airports
- November 2015 Notice (80 FR 70241) Otay Mesa Field Trial
- Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States" Sec. 8. Expedited Completion of the Biometric Entry-Exit Tracking System (March 6, 2017)

4.4 Threats/Hazard Summary

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

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

Table 3, Threats and Threat Avoidance, describes the potential threats, impacts and avoidance objectives based on target capabilities.

Threat Description	Threat Impact	Threat Avoidance Objectives
Establish Identity at Entry and Exit – The inability to establish the true identity of a person entering or exiting the country may allow terrorists or other people of interest or known criminal behavior to enter or remove themselves from the country and continue their nefarious activities. These activities may result in injury or death to many people as well as destruction of public or private property	• Public • Operations • Technical	• Prevent, avoid, or stop an imminent, high risk traveler from performing an actual act of terrorism. • Enhance CBP enforcement policies and operational business processes to remain agile and adaptable in supporting operational requirements to ensure efficiency and effectiveness.

Threat Description	Threat Impact	Threat Avoidance Objectives
and destruction of sensitive data through cyber terrorism or espionage.		• Systemically respond in a timely manner to identify the level of suspected threat of inbound and outbound travelers, protect property and the environment; and prevent acts of terrorism. • Deploy an advanced, integrated, secure technical infrastructure to support advanced identity verification and real-time queries against databases that pre-positions traveler information which will allow CBP Officers to assess quickly, reliably and accurately traveler information prior to exiting the country. • Redesign or reconfigure physical areas and/or operational procedures to support secure processing of detained travelers.
Ensure Departure from the U.S. – The inability to ensure that a traveler has physically departed the country may result in people staying in country who have overstayed their visa or allowing a person to remain in the country when they otherwise should have left.	• Public • Operations • Technical	• Systemically respond in a timely manner to identify the level of suspected threat of outbound travelers, protect property and the environment; and prevent acts of terrorism. • Processing and translating data into meaningful information to determine a suspected traveler's threat level. • Deploy an advanced, integrated, secure technical infrastructure to support advanced identity verification and real-time queries against databases that pre-positions traveler information which will allow CBP Officers to assess quickly, reliably and accurately traveler information prior to exiting the country.
Ensure Protection of Personal Data – Centralized storage and regular transmission of sensitive, personal data impacts the confidentiality, integrity, and availability of biometric PII data which may increase the risk of identity theft and other harm to individuals.	• Public • Technical	• Ensure use of strong end-to-end encryption of all data • Verify information requests to avoid compromise, exfiltration, and exploitation of derogatory information held by the government by an individual or organization seeking to subvert the entry and exit process

Threat Description	Threat Impact	Threat Avoidance Objectives
		• Regularly test systems for vulnerabilities by external and internal threats including auditing of user logs

Table 3—Threats and Threat Avoidance

5 Capability Gap and Overlaps/Redundancies

5.1 Current "As-Is" Capability Assessment

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

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

5.2 Identified Capability Gaps

This section describes necessary capabilities needed to accomplish the biometric entry-exit mission as summarized in Table 4, Capability Gaps.

Capability Gap	Current Capability or Gap?
Verify Traveler Identity	Partial Gap
Create and Manage Biometric Records	Partial Gap
Generate Metrics and Reports	Gap

Table 4 - Capability Gaps

1. Capability Gap #1: Verify Traveler Identity
   a. Capability Description: The ability to capture, review, analyze, search, and match a traveler's biometric information to their biometric and biographic records when entering and exiting the U.S. for the purposes of verifying their identity.
   b. Capability Gap Assessment: Partial Gap, Biographic information is used for identity verification today.
   c. Capability Attribute Description
      i. 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 for quick, reliable and accurate traveler assessment upon entry, or prior to exiting the country.

ii. Operational Measures:

- Percentage of arriving and departing travelers verified biometrically.
- Time to complete traveler verification process from biometric capture to return of biometric matching result.
- Number of travelers processed per minute.
- Traveler wait time in minutes.
- Number and type of overstays/persons of interest identified.

2. Capability Gap #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 Gap Assessment: Partial Gap, No capability exists at exit; biographic and fingerprint information on in scope foreign nationals on entry, no biometrics on U.S. citizens.
   c. Capability Attribute Description
      i. 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.
      ii. Operational Measures:
         - Accurate biometric verification of arriving and departing travelers.
         - Border entry and exit record match.

3. Capability Gap #3: Generate Metrics and Reports
   a. Capability Description: The ability to measure and report the effectiveness of the biometric entry-exit system.
   b. Capability Gap Assessment: Gap, No capability
   c. Capability Attribute Description
      i. 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.
      ii. Operational Measures:
         - System Availability >99%

- System Reliability >99%
- Continuously improving confidence level for matching data consistent with technology enhancements.

5.3 Capability Gap Status

There is a significant gap between the end-state vision and current capabilities. This section addresses the needed capabilities, the current state, shortfalls in capability to achieve mission goals and gap priorities and relationships.

Table 5, Capability Gap Categories, summarizes whether a specified capability supports similar mission areas in multiple DHS components, is intentionally redundant for failover purposes, or provides an opportunity to more efficiently meet DHS and component mission areas.

Capability Gap	**Capability Overlap?[6]**	**Capability Redundancy?[7]**	**Capability Fragmentation?[8]**
Verify Traveler Identity	N	N	Y
Create and Manage Biometric Records	N	N	Y
Generate Metrics and Reports	N	N	N

Table 5—Capability Gap Categories

The capability gaps that have been identified as fragmented are described below.

Capability Gap #1 Verify Traveler Identity: CBP is responsible for traveler identity verification, but dependent upon another organization for biometric matching data.

Capability Gap #2 Create and Manage Biometric Records: CBP is responsible for creating biometric records, but dependent upon another organization for management of biometric data.

5.4 Capability Gap Current and Future Risk

Additional analysis was performed on each identified capability gap to document the current assessment of how addressing each gap would impact risk. The result of this analysis is detailed in Table 6, Capability Gap Future Risk Impact Assessment.

[6] Capability Overlap: Instances when multiple DHS Components, Headquarters elements, offices and/or entities have capabilities with similar goals, support similar activities, or target similar mission needs. [DHS JRIMS Instruction 107-01-001-01]

[7] Capability Redundancy: Instances when additional or alternative capabilities exist across DHS elements, to include those with primary application in other or related mission/functional areas, which maintain a degree of overall functionality in case of loss or failure of another. [DHS JRIMS Instruction 107-01-001-01]

[8] Capability Fragmentation: Instances when capabilities are manifested in multiple DHS Components, Headquarters elements, offices and/or entities to meet the same need and where opportunities exist to more efficiently meet missions, functions, or objectives. [DHS JRIMS Instruction 107-01-001-01]

Capability Gap	Existing Risk	Future Risk Impact
Verify Traveler Identity	The inability to verify the true identity of a person entering or exiting the country may allow terrorists or other people of interest or known criminal behavior to enter or remove themselves from the country posing significant risk to national security.	The ability to verify identity of all travelers entering and leaving the country will significantly reduce the risk of terrorism and criminal activity. The ability to identify all travelers will provide both a deterrent and an improved enforcement posture.
Create and Manage Biometric Records	The inability to create, update, and analyze comprehensive traveler information impacts CBP's ability to assess traveler status, identify and report on overstays, and support enforcement of immigration laws and regulations.	The ability to process entering or exiting travelers using an advanced, integrated, secure technical infrastructure and data that supports identity verification will reduce the risk posed by unknown travelers, unidentified overstays, and improve overall compliance with U.S. immigration policy.
Generate Metrics and Reports	The inability to generate reliable reports limits CBP's ability to define the scope of the problem, effectiveness of current enforcement measures, meet current reporting requirements, and assess operational performance to counter terrorism and advance border security.	The ability to generate accurate, comprehensive reports that support management decision-making will help target resources for more effective operations and enforcement. The ability to create accurate, comprehensive reports will provide senior management and CBP oversight organizations with confidence in CBP's effectiveness and overall capability to support its missions.

Table 6—Capability Gap Future Risk Impact Assessment

5.5 Alignment with DOTmLPF-R/G/S Factors

Currently, there is no one single solution that can fill these capability gaps. CBP has been engaged in a number of biometric field trials that were established to evaluate the ability to capture a biometric identifier and validate a traveler's identity. For example, some of these field trials have included field testing of CBP's ability to compare a live capture facial image with the traveler's passport photo at airports. Another field trial at a land POE evaluated the ability to capture a person's iris and face at entry for comparison when that traveler exited from the U.S. Based on this experience, CBP is prepared to begin identifying solutions that will address each identified capability gap. To enable CBP to further define potential solutions, Table 7 summarizes the identified capability gaps aligned to the DOTmLPF-R/G/S framework. Non-applicable elements of the DOTmLPF-R/G/S framework are not included under the details for each capability gap.

Capability Gaps	DOTmLPF-R/G/S Factors									
	D	O	T	m	L	P	F	R	G	S
Verify Traveler Identity	X		X	X		X	X	X		

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

Table 7—Capability Gap Alignment with DOTmLPF-R/G/S Factors

1. Capability Gap #1 Verify Traveler Identity
   a. Doctrine: While the need to develop a biometric exit system for all travelers leaving the U.S. has been mandated by law (see 1f. Regulations), CBP lacks a clear and approved regulation and policy addressing the collection and use of biometrics on exit.
   b. Training: CBP needs to ensure that CBP officers and staff personnel are trained to collect biometrics correctly.
   c. Materiel: CBP lacks biometric collection equipment to perform biometric matching on departing travelers.
   d. Personnel: CBP lacks the manpower to effectively implement a full departure control system at all air, land and sea locations.
   e. Facilities: CBP will need to ensure that facility constraints at all POEs are included in assessing solution approaches before committing to a certain 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 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.

6 Solution Approach

This solution approach section addresses the three travel modes and the enterprise capabilities that are required to support the end state vision.

As potential solutions are identified to enhance or develop these required capabilities, CBP will assess the suitability, feasibility, and achievability against the following operational issues/considerations:

- Does the solution avoid stove-piped, independent approaches?

- Does the solution use existing physical facilities and infrastructure?
- Does the solution support existing business models and processes?
- Does the solution mirror/emulate/support current behaviors to minimize new or unexpected steps for travelers?
- Does the solution use existing data and IT infrastructure?

As part of the solution approach under this program, CBP is coordinating biometric entry and exit requirements with Office of Biometric Identity Management (OBIM) with the goal to migrate the enterprise facial matching capabilities to OBIM when CBP's requirements can be fully met. CBP and OBIM will jointly develop a roadmap to utilize OBIM's facial matching capabilities starting with performing joint testing. The initial test will take place in Q1 FY 2018 and will provide insight into the feasibility of OBIM's facial matching service supporting CBP's biometric matching needs. CBP will transition to fully utilize OBIM's facial image matching services once OBIM can meet the biometric matching requirements for air, land and sea environments.

In addition to coordination with OBIM, CBP is engaging the Transportation Security Administration (TSA) on biometric exit capabilities and the potential use of CBP or DHS backend services to support traveler identity verification at the check point. TSA will include CBP in their "check point of the future" working group in order to collaborate on biometric exit requirements.

As solution approaches are under consideration, CBP will also seek to ensure compliance with all applicable privacy policies (e.g., Privacy Act of 1974, E-Government Act of 2002), procedures and internal controls necessary to safeguard personally identifiable information (PII) pursuant to the E-Government Act of 2002. In addition, CBP will ensure compliance with all applicable civil rights and civil liberties policies and protections.

6.1 Approach by Travel Mode

Each travel mode offers unique challenges that will require integrated solutions to mitigate any potential impacts to travel. The following sub-sections identify the proposed solution from a user-oriented perspective in operational settings for air, land and sea. All travel modes will use an integrated, enhanced technology environment that will support partners, stakeholders and CBP operations in carrying out the mission.

These solutions for all travel modalities align with CBP's transformative vision to utilize biometrics as an alternative to biographic data as the key to unlocking a traveler's record throughout the travel process. Air is the first priority for implementing biometric entry-exit. Biometric entry-exit solutions for land and sea will follow, leveraging solutions and lessons learned from deployment of an air exit program.

6.1.1 Air Environment

The solution approach for air travel will transform the way CBP identifies air travelers by shifting the key to unlocking a traveler's record from biographic identifiers to biometric ones – primarily a traveler's face. Pre-staging the existing traveler data upstream in the travel process enables all stakeholders to transform from manual and redundant processes to a safer, automated, and seamless traveler movement. CBP can continue to increase security by using a

facial biometric to match the traveler to their advanced passenger information, while simultaneously checking the fingerprints on file against biometric watch lists, which decreases dependency on less reliable paper travel documents, such as passports and visas. This approach will also facilitate traveler movement by providing partners – airlines, airports, and TSA – with a common and unique biometric key for identifying and matching travelers to their identities, creating a more seamless travel experience. CBP will partner with the air travel industry and TSA to deploy a biometric air entry/exit solution that transforms the overall traveler experience. To successfully implement this solution, CBP will accomplish the following:

1) Re-engineer and re-design CBP data handling;
2) Build a backend communication portal to connect with partners;
3) Develop new inbound software that leverages one-to-many biometric searching; and,
4) Implement a mechanism to provide wayfinding and lane assignments prior to entry.

If further testing shows that a token-less approach is found not to be viable for performance reasons, CBP will revert to a solution that utilizes a token (e.g., a boarding pass or travel document) to perform a 1:1 biometric facial or fingerprint recognition match of the traveler departing, which will increase operational complexity and processing times.[9]

6.1.2 Land and Sea Environments

As stated in Section 1 and 2 the capability needs in this CAR apply to air, land, and sea environments. Due to mission priorities CBP has prioritized the entry-exit capability development by travel mode—air, land, and sea. This approach allows CBP to effectively plan and schedule so that CBP can address future needs in a logical manner. CBP's top priority for deployment of biometric entry-exit capabilities is in the air environment, followed by land and sea. Due to the initial focus on the air environment solution approaches, CBP will assess solution approaches for the land and sea environment in subsequent analyses leveraging what is learned in the air environment along with additional operational field tests.

6.2 Enterprise Solutions

6.2.1 Technology Support

The program is working with the CBP Office of Information and Technology (OIT) to establish a comprehensive, scalable solution to meet the future need for real-time access to data and storage volumes that will be required to support biometric data. Biometric entry-exit will use current IT capabilities and work with OIT to develop scalable approaches, potentially to include COTS cloud-based solutions, until such time that a full architectural design for an enterprise technology solution can be developed, acquired and supported. CBP is working with OBIM to identify biometric data storage and biometric matching solutions that addresses CBP's capability needs.

6.2.2 Physical Infrastructure

The physical infrastructure imposes a constraint on available solution options. CBP will partner with relevant stakeholders to leverage existing infrastructure within the POE to process

[9] A 1:1 biometric "verification" authenticates a traveler's identity by comparing a captured biometric with a biometric template pre-stored in a database.

travelers of interest and to ensure the safety of the officers and the traveling public. If at a specific POE, the current physical infrastructure is insufficient, then CBP will work to identify other solution approaches that mitigates the risk to officer and traveler safety while enabling enforcement and facilitation activities.

6.2.3 Outbound Enforcement

Biometric entry-exit will also include new outbound enforcement regulations and policy specifically focused on those violations that warrant an enforcement action for an individual departing the U.S. If any threats are identified at the time of boarding a flight departing the U.S., the biometric entry-exit system will alert CBP outbound enforcement teams by sending a message to their mobile device. Teams will respond to adjudicate the issue. Outbound policy will address how to resolve non-law enforcement related exceptions such as failure to capture a live biometric image and failure to match to biometric images of expected travelers on the flight manifest. The system will also have the capability to inform the airline, or a third party, if the traveler has matched their biometrics successfully. Efforts are also underway to determine the key regulatory requirements for PII in a biometric world. The results of these efforts will drive the detailed implementation solution(s). Coordination with relevant law enforcement authorities will occur as per existing standard operating procedures (e.g., Immigration and Customs Enforcement (ICE), local Police Departments.)

7 CAR Checklist

Capability Analysis Report (CAR) Checklist			
Item	**Criteria Importance**	**Criteria**	**Assessment (Met/Not Met)**
1	CRITICAL	Is the CAR signed by the requisite parties?	
2	NON CRITICAL	Does the executive summary contain necessary salient points?	
3	CRITICAL	Does the CAR document the scope of the assessment in alignment with the study plan?	
4	CRITICAL	Does the CAR properly describe the capabilities in functional terms?	
5	CRITICAL	Does the CAR provide traceability between strategic guidance; operational missions, objectives, or function; threat and hazards; and requirements?	
6	CRITICAL	Does the CAR provide traceability of those missions, functions and/or operations to relevant parts of Departmental strategic guidance, plans, concepts and/or other relevant factors to which the identified necessary capabilities contribute?	
7	CRITICAL	Does the CAR identify the threats and hazards associated to the mission, function, or objective?	
8	CRITICAL	Are the necessary capabilities defined and in alignment with the strategic guidance, threats, hazards, and operational views?	
9	CRITICAL	Does the CAR define a standard for the measures and metrics used to evaluate the capability effectiveness and success in achieving the desired outcome?	
10	CRITICAL	Does the CAR establish the "as-is" baseline for the capabilities?	
11	CRITICAL	Does the CAR identify the capability gaps related to proficiency, sufficiency, lack of fielded capability, age of fielded capability, or non-materiel reasons?	
12	CRITICAL	Does the CAR identify overlaps, redundancies, and fragmented capabilities?	

Capability Analysis Report (CAR) Checklist			
Item	**Criteria Importance**	**Criteria**	**Assessment (Met/Not Met)**
13	CRITICAL	Are the existing and future risks associated with each gap assessed?	
14	CRITICAL	Does the CAR identify non-materiel alternatives following the Doctrine, Organization, Training, materiel, Leadership/Education, Personnel, Facilities categories?	
15	CRITICAL	Does the CAR identify materiel alternatives if non-materiel alternatives do not close the gaps?	
16	CRITICAL	Does the CAR assess the non-materiel alternatives against suitability, feasibility, or achievability?	
17	CRITICAL	Does the CAR assess the materiel alternatives against suitability, feasibility, or achievability?	