Transportation Security Administration

TSA BIOMETRICS STRATEGY

For Aviation Security & the Passenger Experience

July 2018

TABLE OF CONTENTS

LETTER
FROM THE ADMINISTRATOR

I am proud to present the Transportation Security Administration's Biometrics Strategy for Aviation Security and the Passenger Experience. This strategy will guide our efforts to modernize aviation passenger identity verification over the coming years.

This document aligns with and supports the 2018-2026 TSA Strategy I announced earlier this year in several ways. It defines clear pathways to improve security, safeguard the Nation's transportation system, and accelerate the speed of action through smart investments and collaborative partnerships.

To achieve the vision, goals, and objectives outlined in the Biometrics Strategy, TSA will leverage innovative biometric concepts and solutions that will enhance security effectiveness, improve operational efficiency, and yield a consistent, streamlined passenger experience in coordination with our aviation security partners.

In addition to addressing key operational needs, implementing the biometrics strategy will secure TSA's position as a global leader in aviation security and advance global transportation security standards.

I want to thank everyone at TSA, our interagency partners, and industry stakeholders – including airlines, airports, and solution providers – who provided input to develop this strategy. It represents the beginning of an important and exciting conversation that I look forward to continuing with you as we execute the TSA Biometrics Strategy.

David P Pekoske

David Pekoske
Administrator
Transportation Security Administration

Executive Summary

Identity verification is a cornerstone of TSA's operational landscape in the commercial aviation sector. In order to meet the challenges of evolving security threats, rising air travel volumes, resource constraints, and limits on operational footprint, TSA and aviation security regulators around the globe must look to automate manual and paper-based identity verification processes through smart technology investments. The TSA Biometrics Strategy lays out a practical approach to leverage biometric technologies to improve security effectiveness and operational efficiency while also enhancing the passenger experience.

TSA is stepping into the biometric solution space at an ideal time to capitalize on technological advancements in biometric system accuracy, speed, and ability to automate high-throughput operations. Additionally, traveler sentiment toward biometric technologies has evolved toward appreciation for the enhanced security and efficiency they can provide.

The TSA Biometrics Strategy incorporates feedback gathered during more than forty targeted engagements with strategic aviation security leaders from airlines, airports, and solution providers. Feedback was also gathered from key government stakeholders, including TSA internal offices, DHS headquarters and operational Components.

The strategy articulates a collaborative biometric vision for TSA and its aviation security partners in the context of an overall identity verification and management approach. The vision is achievable through the alignment and parallel advancement of four strategic goals and associated objectives. The TSA Biometrics Strategy describes the "what" and the "why" of TSA's biometric approach. Implementation plans will be developed to describe the "who, when, and how." Implementation of each goal and associated objectives will be shaped by a set of clear guiding principles listed in Figure 1.

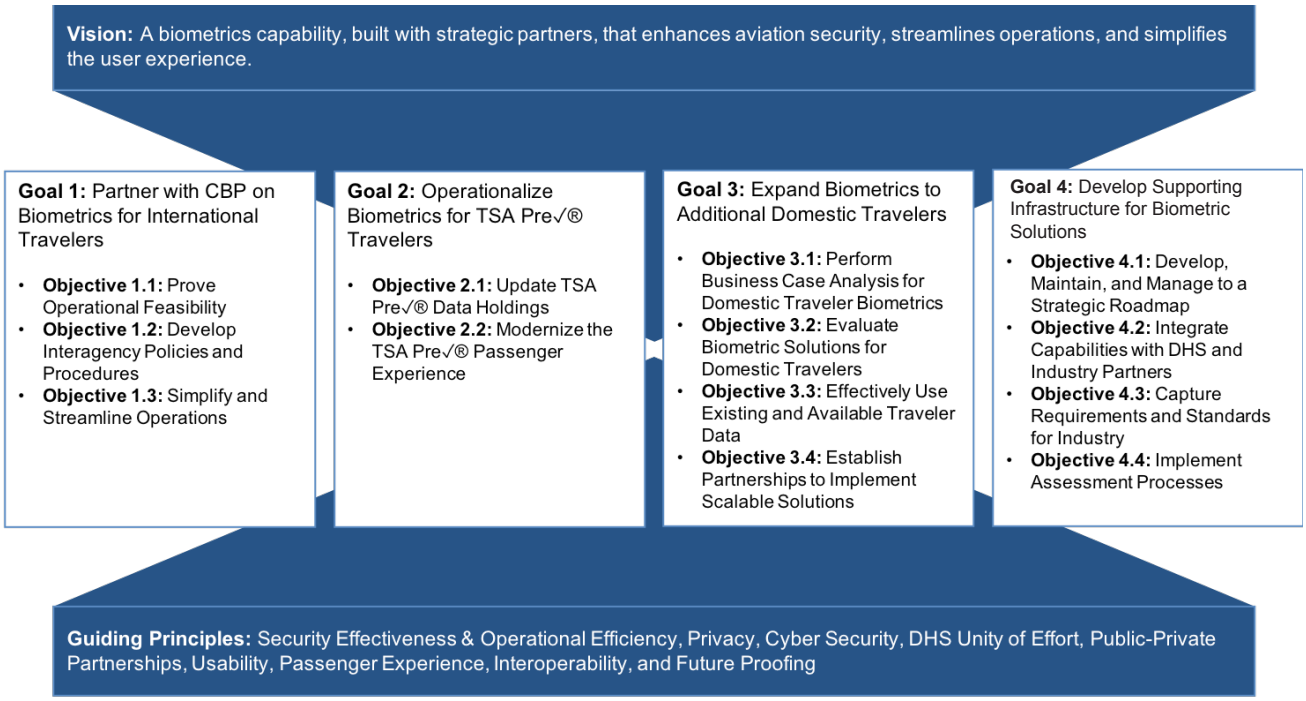


FIGURE 1 TSA Biometrics Strategy

I. Purpose & Scope

This document articulates a strategy for TSA to leverage biometric solutions to increase security effectiveness while also improving operational efficiency and the passenger experience. Due to the growing volume of commercial aviation passengers TSA screens – more than two million per day – this initial release of the TSA Biometrics Strategy is focused on verifying aviation passenger identity using biometrics per TSA's authorities under applicable laws and regulations including the Aviation and Transportation Security Act (Section 109 (a)(7)). Over time, passenger-centric solutions can be extended to other key groups such as aviation workers, law enforcement officers, and known crew members.

TSA will continue to use facial images as the primary means of identity verification for aviation security screening. Facial recognition capabilities will be automated to improve the performance and security of TSA operations by increasing assurance of traveler identity beyond what travel documents alone can provide. Fingerprints will continue to serve as the primary biometric modality for trusted traveler and other credentialed enrollments and security threat assessments. In the future, multi-modal approaches may help further increase accuracy, security, and scalability.

Facial recognition has long been TSA's modality of choice in aviation security operations. Today, TSOs and airline employees manually compare the passenger in front of them to their photo ID. The TSA Biometrics Strategy seeks to leverage facial recognition technology to automate that process to enhance security effectiveness, improve operational efficiency, and streamline the passenger experience.

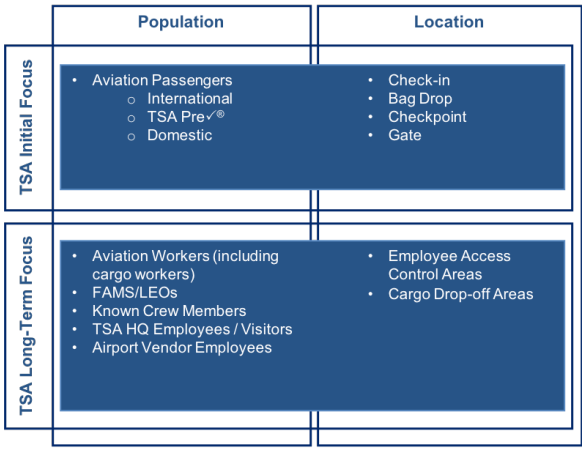


FIGURE 2 Scope of TSA Biometrics Strategy

Today, facial recognition provides TSA with several key benefits. Facial recognition systems can be self-service, facilitative and incorporate anti-tampering countermeasures, enabling TSA and aviation security partners to reduce reliance on physical travel documents and manual inspection. Facial recognition benefits from the wide availability of high-performance, low-cost, and commercially available camera systems that could be extended, in collaboration with aviation security partners, across the entire passenger experience from reservation to boarding.

Additionally, Federal and state identity document issuance organizations already collect facial images that are generally suitable for facial recognition capabilities. Biometric data for fingerprint or iris recognition are generally not available for the majority of travelers. Face image standards are widely adopted and used throughout civil aviation for identity verification per International Civil Aviation Organization Doc 9303.

II. Strategic Drivers

Biometric technology pilots over the past two years have shown the potential for biometrics to close capability gaps in current operations. Additionally, the conclusions stated in a recent TSA capability analysis report further solidified the need to establish a strategy for implementing biometric solutions. Recognizing the need for TSA to take a more comprehensive approach, the Administrator tasked the development of the Biometrics Strategy in April 2018. Over a three-month period, TSA engaged a wide range of stakeholders across DHS Headquarters, DHS Operational Components, and industry to solicit their input and feedback on the development of the TSA Biometrics Strategy. Dialog with interagency partners, airlines, airports, and solution providers yielded additional insights into the forces driving the adoption of biometrics in the commercial aviation sector. TSA's implementation of biometric solutions will take shape within the context of these forces and takes them into consideration.

Current Operations

To achieve its mission of protecting the Nation's transportation systems to ensure freedom of movement for people and commerce, TSA must be able to effectively screen individuals seeking to board aircraft in the sterile area of U.S. airports. Today, TSA and airline partners verify traveler identity primarily through the processing of biographic data and the inspection of physical identity and travel documents to ensure the passenger presenting themselves at the airport is the same person who was pre-screened based on biographic data. In the near term, TSA will deploy Credential Authentication Technology (CAT) which will automatically verify the authenticity of passengers' credentials (e.g., driver's license, passport) and allow Transportation Security Officers (TSOs) to verify passenger pre-screening status in near-real time. TSA can further enhance its security posture by combining the power of credential authentication and biometric identity verification , particularly for facial matching solutions that rely upon the use of valid physical identity credentials.

> "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 in the security market today include fingerprints, facial image, or iris scans."
>
> - DHS Biometrics Strategic Framework 2015-2025

Technological Advancement

The pace of change in the biometric marketplace continues to accelerate. Once limited to more narrow physical access control applications, biometrics have gone mainstream. Standardization, commoditization, the rise of machine learning, and the wider availability of biometric matching algorithm training data – particularly facial images – has led to an explosion of competition and solution offerings. Today, technological solutions for identity verification provide much improved speed and accuracy that generally exceed human capabilities. TSA's exploration of biometric solutions comes at an ideal time to capitalize on recent advances.

Cultural Shift

Travelers increasingly use biometrics such as fingerprint and facial recognition in their daily lives to access their mobile devices, apps, and accounts. As biometric usage continues to spread throughout the consumer market, popular perceptions have evolved to appreciate the convenience and security biometric solutions offer in the commercial aviation sector.[1] TSA can learn from this trend and adopt solutions that enhance security and address traveler demand for self-service options that minimize direct interaction with government and airline personnel.

1 OAG Travel Tech Innovation: Market Report, Evaluating Travelers' Appetite for Adoption

Rising Travel Volume

Airlines, airports, and security regulators around the globe, like TSA, are faced with an ever-rising volume of air travelers to facilitate and screen. Meanwhile, personnel staffing growth is flat or declining and physical infrastructure/footprint remains relatively static, particularly in airports where capital improvement projects require long lead times. If unaddressed, rising travel volume combined with operational constraints will result in longer wait times and more missed flights. Neither the aviation industry nor the government can staff its way out of this challenge. Both must look to innovative concepts and technologies like biometrics to improve both security effectiveness and operational efficiency.

Emerging Business Case

Airlines and airports prioritizing their investments have expressed strong interest in streamlining and modernizing the passenger experience from curb-to-gate or even reservation-to-destination. Some aviation industry stakeholders are leaning forward and submitting security procedure amendments (e.g., for biometric bag drop) while others position themselves as "fast followers." CBP's biometric Air Exit program has proven the aviation industry is willing to invest in joint solutions if the business case is clear. Current and projected resource constraints underline the need for TSA to follow a similar approach, one that fully unlocks the biometric business case by prioritizing collaborative partnerships with interagency and industry partners.

III. Biometrics Vision

In the coming years, TSA will seek to achieve a vision for biometrics that will fundamentally transform security operations and the passenger experience across the Nation's commercial aviation ecosystem.

"A biometrics capability, built with strategic partners, that enhances aviation security, streamlines operations, and simplifies the user experience."

IV. Strategic Goals & Objectives

TSA will achieve its biometrics vision for all commercial aviation travelers by advancing four strategic goals and associated objectives in parallel. TSA will:

1 Partner with CBP on Biometrics for International Travelers

2 Operationalize Biometrics for TSA Pre✓® Travelers

3 Expand Biometrics to Additional Domestic Travelers

4 Develop Supporting Infrastructure for Biometric Solutions

TSA will develop implementation plans and roadmaps to actualize each of the strategic goals and objectives in a practical, time-bound manner. Implementation plans will capture dependencies, owners, stakeholders, and detailed plans of action. Recognizing there is no turn-key biometric solution for all travelers today, TSA and its strategic security partners will take a phased approach to implementation that incrementally builds upon credential authentication capabilities to incorporate biometric identity verification. This approach will iteratively build capability and reduce operational friction over time by automating manual processes, preserving resilient fail-over systems, and introducing biometric matching services across international passengers, trusted travelers, and the general domestic passenger population in accordance with applicable laws, authorities, and privacy considerations.

Through the Secure Flight program, TSA has the benefit of knowing which travelers are likely to appear at any airport on a given day. This provides an opportunity for TSA to use passenger pre-screening status to pre-stage biometric data, in this case facial images, for verifying passenger identity in 1:1 and/or 1:N modes of operation. In the case of international passengers, TSA can leverage DHS and other Federal sources for facial images of foreign visitors and U.S. citizen passport holders.

1:1 Matching:
Compares a live image capture of a subject (i.e. the passenger) against a single record (e.g., his/her passport photo). The record may reside on a travel document like a passport or in a database.

1:N Matching:
Compares a live image capture against a number (N) of records ranging from a subset (e.g., 300 passenger flight) to the entire enrolled population in the reference database.

In the future, TSA Pre✓® will similarly be able to call up facial images of voluntarily-enrolled applicants. For the majority of travelers who are flying domestic itineraries and do not have a passport photo on file, TSA will explore innovative opt-in approaches to building biometric capabilities consistent with the international and TSA Pre✓® passenger experience as well as applicable statutes and privacy protections.

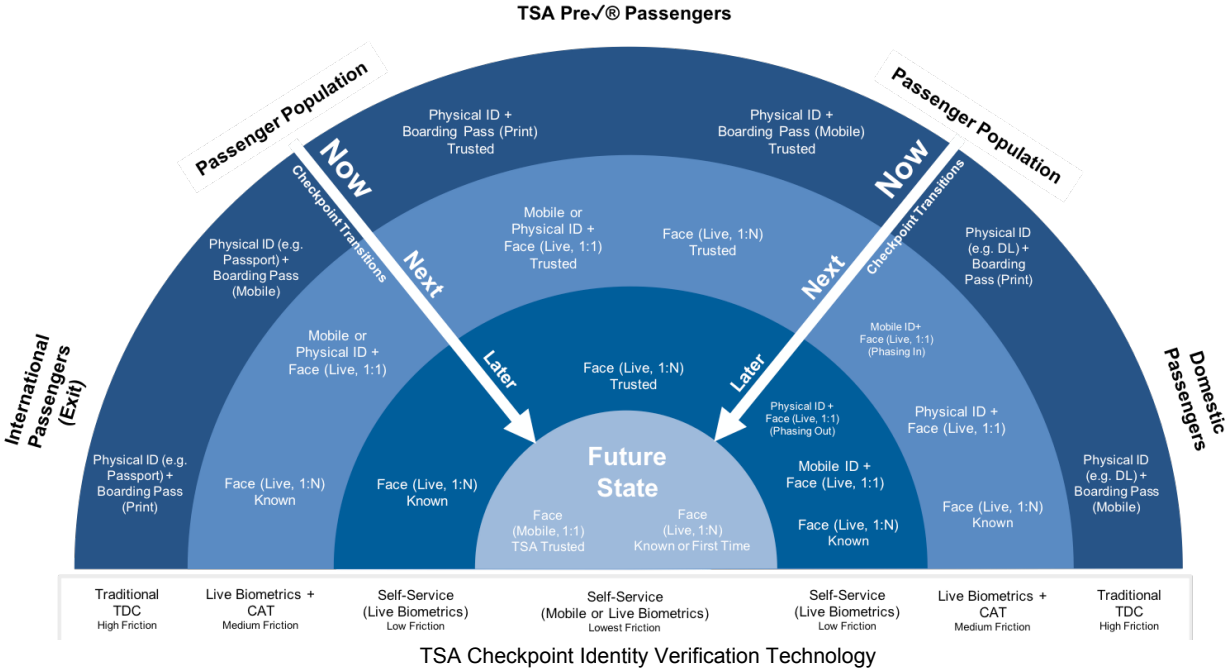


FIGURE 3: Notional Phased Approach to TSA Checkpoint Identity Verification Future State

1

Partner with CBP on Biometrics for International Travelers

In recent years, CBP has invested significant financial and technical resources to develop a biometric Air Exit capability to fulfill Congressional and Executive branch mandates to biometrically verify the departure of foreign nationals from the United States. While CBP and TSA requirements will differ in some regards, the biometric Air Exit program offers both operational Components the opportunity to demonstrate DHS Unity of Effort and conduct joint operational pilot projects, data collection, solution refinement, and data exchange. This effort will also enable TSA to identify and examine technical, legal, and regulatory issues to consider prior to broader deployment.

Objective 1.1: Prove Operational Feasibility

TSA and CBP will continue piloting efforts currently underway to implement facial recognition for identity verification of international travelers transiting TSA checkpoints.[2] TSA and CBP, in coordination with Office of Biometrics and Identity Management (OBIM), will continue to build on recent efforts to develop, design, and execute pilot projects at checkpoints that streamline and automate all or part of the Travel Document Checker (TDC) process and satisfy CBP's biometric Air Exit requirements. CBP and TSA will focus on continuing current pilot projects and conducting additional biometric technology pilots at locations where airport and airline stakeholders have committed to making their own investments to streamline the passenger experience using facial recognition technology. Travelers will be notified of pilot project activities and have the ability to opt-in to various biometric procedures. TSA and CBP will analyze biometric technology pilot results and refine approaches for future efforts.

Objective 1.2: Develop Interagency Policies and Procedures

Alongside the phased pilot projects, TSA and CBP will develop joint policies and standard operating procedures for biometric screening of international passengers transiting through TSA checkpoints during operational pilots as well as operations at scale. CBP and TSA will work together to develop a plan ensuring CBP Officers can be co-located at TSA checkpoints to perform biometric exit exception processing and any resulting law enforcement functions, as appropriate under CBP and TSA authorities. As TSA checkpoints are upgraded to accommodate biometric technology, TSA and CBP will work to limit the impact to passenger wait times and TSA operations. TSA and CBP will develop a concept of operations, standard operating procedures, and policies related to these efforts for review by counsel, privacy officials, and senior leadership of both agencies.

Objective 1.3: Simplify and Streamline Operations

TSA and CBP will work to integrate similar functions and capabilities to enable scaled, automated, and streamlined operations in the future. TSA and CBP will collaborate with DHS Science & Technology (S&T) to ensure facial matching capabilities are optimized for the larger gallery sets needed for checkpoint processing. Together, as biometric matching continues to mature, TSA and CBP will work with OBIM to create an integration roadmap to the Homeland Advanced Recognition Technology (HART) in accordance with DHS guidance and policy. As the Congressionally-designated lead provider of biometric identity services for DHS, OBIM serves a critical function by enabling CBP and TSA missions through biometric matching, storing, sharing, and analysis. DHS achieves both mission benefit and efficiencies through a centralized biometric service provider and data store.

2 Joint TSA/CBP Policy on Use of Biometric Technology, signed April 2018

2

Operationalize Biometrics for TSA Pre✓® Travelers

Today, the TSA Pre✓® Application Program collects fingerprints from applicants to conduct criminal history checks as part of its enrollment and security threat assessment process. Through this process, TSA can be confident in issuing a known traveler number (KTN) to vetted applicants which they can then provide to an airline during the reservation process, receive a boarding pass, and enter the TSA Pre✓® screening lane at the airport. Moving forward, TSA Pre✓® will increase its access to and utilization of voluntarily-provided biometric data, including facial images, to modernize the trusted traveler experience for TSA Pre✓® travelers.[3]

3 In this context, TSA Pre✓® travelers include all trusted travelers for whom a facial biometric image is or will become available, including members of the TSA Pre✓® Application Program, members of the CBP Global Entry program, and other trusted traveler populations.

Objective 2.1: Update TSA Pre✓® Data Holdings

In calendar year 2019, the TSA Pre✓® Application Program will transition from single-factor enrollment to multi-modal (fingerprints + facial) enrollment for new applicants in calendar year 2019. Additionally, TSA will seek to supplement data of currently enrolled TSA Pre✓® members and incorporate additional truster traveler populations by leveraging similar systems that are also used to enroll and verify traveler identities such as State Department passport photos and CBP's Global Entry program. In addition to exploring ways to In addition to exploring ways to update current data holdings and increase enrollment rates increase enrollment rates, TSA Pre✓® will identify, test, and evaluate innovative methods (e.g., online, in airport) of collecting biometric facial images from re-enrollees without sacrificing the security and integrity of the program (e.g., more mobile technology, expanding in-airport and other flexible enrollment access capabilities). TSA will integrate existing biometric holdings and newly-collected biometric data with the DHS enterprise biometric system of record (IDENT/HART) and gain access to additional biometric services in accordance with applicable laws, regulations, and policy.

Objective 2.2: Modernize the TSA Pre✓® Passenger Experience

TSA will go beyond biometric enrollment to further secure, facilitate, and enhance the TSA Pre✓® passenger experience. In partnership with industry, interagency, and intra-departmental partners (e.g., DHS S&T), TSA will evaluate alternative concepts of operation and technologies for streamlining and enhancing the TSA Pre✓® product while ensuring a consistent passenger experience across all lanes.

3

Expand Biometrics to Additional Domestic Travelers

TSA will seek new and innovative approaches to extend opt-in biometric solutions to the general flying public by exploring a range of options for enabling a secure, scalable, biometric passenger experience.

Objective 3.1: Perform Business Case Analysis for Domestic Traveler Biometrics

TSA will partner with OBIM and other strategic partners to research and evaluate options to secure and facilitate travel for non-TSA Pre✓® domestic travelers using opt-in biometric capabilities. Many if not most of these travelers do not have biometric data on file with the U.S. government (e.g., a passport photo), posing a unique challenge for TSA and its strategic security partners. An assessment of authorities, privacy issues, costs, tradeoffs, and potential, phased courses of action will inform the solution space as TSA assesses ways to improve the screening experience for the domestic passenger population.

Objective 3.2: Evaluate Biometric Solutions for Domestic Travelers

TSA will conduct pilot projects and evaluate innovative concepts with industry and interagency partners (e.g., CBP, DHS S&T, OBIM) including token- and token-less solutions.[4] TSA will work with CBP and OBIM to examine options to leverage the CBP TVS biometric matching service, IDENT/HART, and other capability options for matching voluntarily-provided domestic passenger facial biometric data within DHS, TSA, and CBP authorities. Additionally, TSA will prepare for the potential acceptance of mobile drivers' licenses (mDL) which several state issuance authorities are beginning to securely provision onto driver's mobile devices in addition to issuing a physical license. These REAL ID compliant identification mediums include biometric images that TSA may be able to leverage for identity verification. As part of this preparation, TSA will consider the impact, if any, of the REAL ID Act on TSA acceptance of mDL at aviation security touchpoints across the passenger experience.

Objective 3.3: Effectively Use Existing and Available Traveler Data

TSA will explore opportunities to more effectively use existing information within DHS systems including DHS databases (e.g., IDENT/HART), State Department passport photos, and solutions that may broker verification touchpoints between federal and state systems. TSA will develop the policy and/or legislative case for the necessary authorities to bolster and best serve domestic passenger biometric data and usage.

Objective 3.4: Establish Partnerships to Implement Scalable Solutions

TSA will develop clear pathways to partnership and collaboration with strategic aviation security stakeholders including airlines, airports, and registered traveler program providers. Due to projected financial and resource constraints, innovative models of public-private partnership will be key to implementing scalable solutions. TSA's approach will be informed by CBP's model for biometric Air Exit by providing vetted industry partners a platform, services, and interfaces to adhere to for the purposes of improving aviation security.

4 A token is any artifact (e.g., boarding pass, driver's license, mobile phone) used to initiate a biometric operation

4

Develop Supporting Infrastructure for Biometric Solutions

TSA will build the strategic, architectural, policy, requirements, and process infrastructure needed to support the multi-pronged capability delivery strategy outlined in Goals 1-3.

Objective 4.1: Develop, Maintain, and Manage to a Strategic Roadmap

In consultation with stakeholders, TSA will lay out a strategic roadmap of the four strategic goals and associated objectives. It will identify key touchpoints within and between the goal workstreams to clearly map out process, technical, and policy dependencies. The strategic roadmap will align with overarching TSA and DHS strategies and guidance including the TSA Pre✓® strategic plan and DHS-wide transition to enterprise biometric services offered by OBIM's HART system.

Objective 4.2: Integrate Capabilities with DHS and Industry Partners

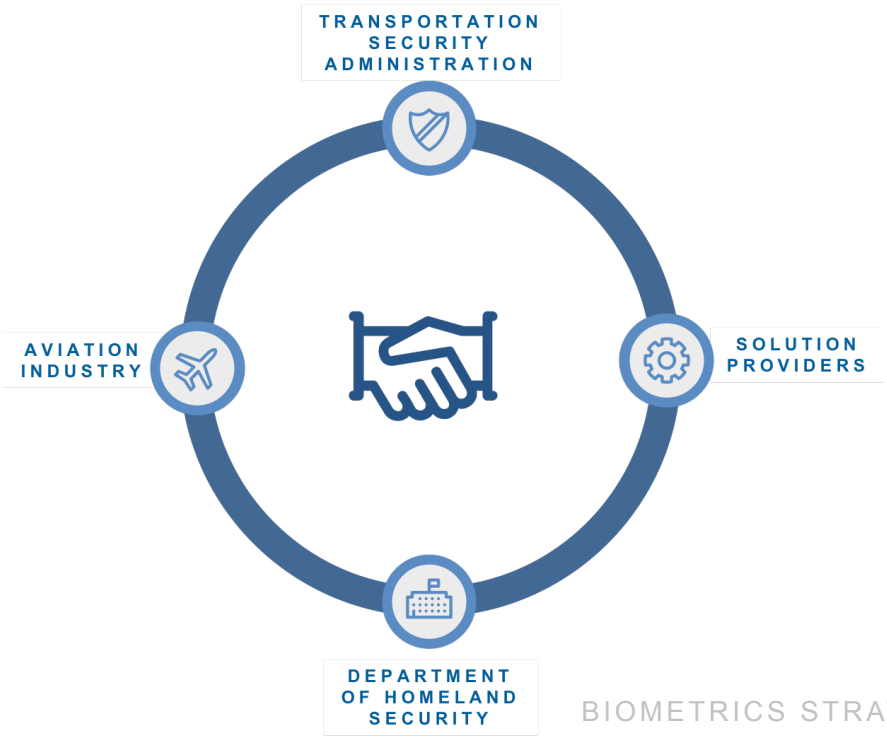
TSA will identify pathways to appropriately leverage existing capabilities and services across TSA, DHS, other Federal agencies, and third parties to accommodate a variety of front-end concepts and solutions. Likewise, TSA will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touchpoints of the passenger experience.

Objective 4.3: Capture Requirements and Standards for Industry

TSA will work with industry partners to define requirements, interfaces, and standards for aviation security touchpoints across the passenger experience (e.g., bag drop, checkpoint) against the backdrop of aviation stakeholders' regulatory obligations to verify passenger identity. Solution providers and aviation security partners will benefit from stable requirements (e.g., for passenger throughput) and common standards for accuracy, throughput, data exchange, and cybersecurity. Interfaces and standards for front-end solutions will enable an extensible, future-proofed architecture to support a variety of concepts and processes.

Objective 4.4: Implement Assessment Processes

TSA will identify, develop metrics, and implement standard assessment processes for proposed biometric solutions. This will enable TSA to quickly evaluate security procedure amendments, assess cybersecurity posture, develop qualified product/service lists, and implement audits and controls to ensure operations are compliant with applicable law and policy.



V. Guiding Principles

In order to make its biometric vision a reality, TSA will adopt a set of overarching core principles, informed by stakeholder feedback, to guide the implementation of the strategic goals and objectives.

Security Effectiveness & Operational Efficiency

Biometrics offer TSA the rare opportunity to increase both security effectiveness and operational efficiency simultaneously, disrupting the historical trade-off between the two. TSA, in coordination with strategic security partners, must implement solutions that take full advantage of this opportunity while also recognizing that identity verification occurs within a complex system of systems. Biometrics can automate current manual procedures and enable reinvestment of screening personnel into performing other critical security tasks and biometric error resolution. In the future, improved screening processes may enable a connection between identity verification and providing x-ray screening of passengers and their carry-on property based on their pre-screening status.

Privacy

TSA will adopt a "privacy by design" mindset that incorporates privacy considerations into each phase of biometric solution development (design, build, implement). Privacy protections will include restrictions to prevent the use of biometrics for purposes other than transportation security unless individuals have opted into other uses.

Cybersecurity

Biometric solutions must be designed to protect data at rest and in-transit to protect both passengers and the integrity of the system across the data lifecycle. Capabilities must adhere to existing and evolving DHS and TSA security requirements as well as industry best practices to enforce cybersecurity compliance.

DHS Unity of Effort

TSA must leverage existing relationships, information, and programs both internally and across DHS. Biometric solutions will build upon the biographic backbone of TSA's current credential authentication, identity verification, and pre-screening systems such as TSA Pre✓®, Secure Flight, and CAT as well as the connective network and "integration fabric" that TSANet and the Security Technology Integration Program (STIP) provide today.

Externally, TSA will partner closely with CBP and other DHS components to align biometric efforts to the overarching DHS Biometrics Framework with the ultimate goal of leveraging OBIM's HART system, the successor to IDENT as well as the biometric repository and matching service for the Homeland Security Enterprise. TSA must also continue to deepen its engagement with DHS S&T and utilize its deep industry knowledge and biometric research, development, testing and evaluation capabilities to

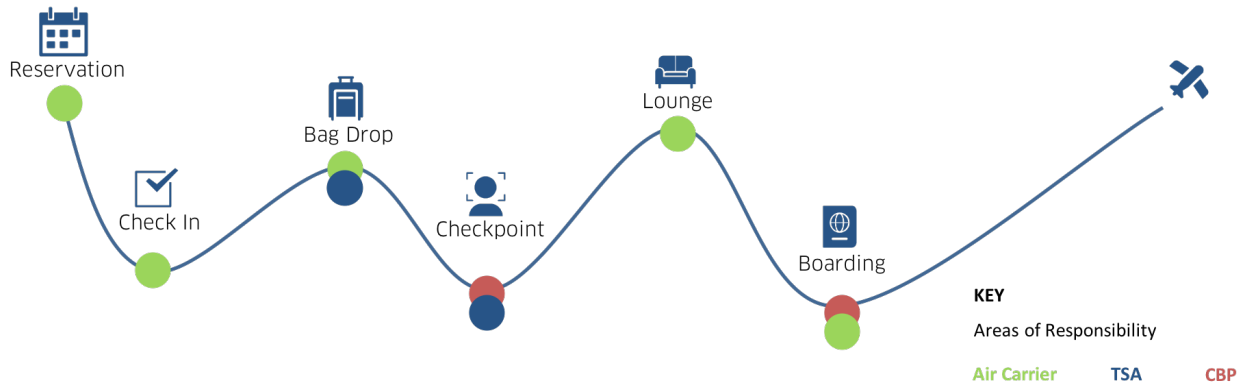


FIGURE 4 Notional Passenger Experience Stakeholder Roles and Responsibilities

explore innovative concepts and technologies prior to field testing or deployment.

Public-Private Partnership

TSA intends to pursue innovative models of public-private partnerships to drive collaboration and co-investment. Leveraging and deepening existing security partnerships with aviation security stakeholders provides the best route to unlocking the business case for a biometrically-enabled curb-to-gate passenger experience. At the same time, TSA and its partners must work to clearly articulate public and private sector roles and responsibilities in the context of applicable laws and regulation.

Usability

Biometric solutions must be highly usable for all passengers and operators taking into account the diversity of the traveling public and TSA Officer roles. Regardless of physical ability, age, gender, skin color, beliefs, disability of medical condition, or other characteristics, passengers and TSOs should be able to successfully interact with the technology or a reasonable alternative concept of operations whether in the form of kiosks, fixed infrastructure (e.g., e-gates), or mobile solutions. TSA and its security partners must be able to achieve high-biometric accuracy rates and improve overall security effectiveness without a disparate and unintended impact on any particular group or groups of travelers. Furthermore, usability has been shown to be a key driver of overall system performance. Usable solutions, engineered with human factors and Officer performance in mind, will result in higher security effectiveness and system performance.

Passenger Experience

Biometrics for aviation security must enable a streamlined and consistent passenger experience across TSA Pre✓® and Standard lanes for both international and domestic travelers. To do so, TSA must harmonize its passenger-facing biometric capabilities with its mission partners, the aviation industry, and global standards with facial recognition as the common denominator for the foreseeable future.

Interoperability

TSA biometric solutions must be compatible with current TSA systems and processes, interoperable with mission partner systems (e.g., CBP, OBIM), and maximize the use of secure and accessible interfaces to facilitate the exchange of biometric data across stakeholders. Support for various data types, versions, and structures should not favor any particular vendor or solution set. Some airlines and airports are willing to collect images, transmit data, and receive matching results on passenger biometrics but may be reluctant to store them due to cost or risk. At the same time, TSA should support solutions that enable the use of passenger biometrics across all airlines and airports rather than proprietary solutions.

Future Proofing

In addition to being consistent and interoperable, TSA's biometric capability must be future proof. It should be upgradeable and extensible across the passenger experience as technical innovation expands the art of the possible. TSA and its security partners must develop an integrated architectural approach to implement modularized, interoperable, and increasingly cost-effective solutions that embrace standards, current and evolving infrastructure, and innovations (such as Cloud) while also maintaining a robust cybersecurity posture.

The underlying architecture should promote flexibility and upgradeability to support an evolving solution space, enable future operational pilot projects, and allow for downstream data analytics in addition to integration of future emerging technologies. Additionally, as biometric technology continues to improve, TSA may wish to incorporate multi-modal biometric verification capabilities to further improve accuracy, security, and scalability.

VI. Moving Forward

The execution of the TSA Biometrics Strategy will start by identifying sponsors for the strategic goals and corresponding objectives. Ongoing efforts and biometric technology pilots will be aligned and continue while implementation plans and roadmaps are developed in consultation with TSA, DHS, Federal, and aviation industry stakeholders. This will require the collective support and dedication of all parties to make the TSA Biometrics Vision a reality.

Appendix A: Terms & Acronyms

Acronym	Term
1:1	One-to-One Matching
1:N	One-to-Many Matching
CAT	Credential Authentication Technology
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
HART	Homeland Advanced Recognition Technology
IDENT	Automated Biometric Identification System
mDL	Mobile Driver's License
OBIM	Office of Biometrics and Identity Management
P3	Public Private Partnerships
S&T	DHS Science & Technology Directorate
STIP	Security Technology Integration Platform
TDC	Travel Document Checker
TSA	Transportation Security Administration
TSO	Transportation Security Officer
TVS	Traveler Verification System

Appendix B: Strategic Alignment

Strategic Alignment		
Document Name	Organization	Sign Date
DHS Biometric Framework	DHS	June-15
TSA Strategic Five-Year Technology Investment Plan (Biennial Refresh)	TSA	Dec-17
TSA Strategy 2018-2026	TSA	Feb-18
TSA Pre✓® Strategic Plan	TSA	June-18
CBP Biometrics Strategy, 2016	CBP	Dec-16

Appendix C: Stakeholders Consulted

Stakeholder Name	Stakeholder Alignment
Department of Homeland Security (DHS) Joint Requirements Council (JRC)	Government
DHS Office of Program Accountability and Risk Management (PARM)	Government
DHS Science & Technology (S&T) Directorate	Government
DHS Office of Biometric Identity Management (OBIM)	Government
TSA Internal Stakeholders (Various)	Government
U.S. Customs and Border Protection (Various)	Government
U.S. Citizenship and Immigration Services (USCIS)	Government
American Association of Motor Vehicle Administrators (AAMVA)	Government
Dallas/Fort Worth International Airport (DFW)	Airport
Los Angeles International Airport (LAX)	Airport
Minneapolis-St Paul International Airport (MSP)	Airport
Orlando International Airport (MCO)	Airport
American Association of Airport Executives (AAAE)	Industry Association
Airports Council International – North America (ACI-NA)	Industry Association
Airlines for America (A4A)	Industry Association
International Biometrics Industry Association (IBIA)	Industry Association
Southwest Airlines	Airline
United Airlines	Airline
American Airlines	Airline
Delta Airlines	Airline
JetBlue Airlines	Airline
Technology Vendors (Various)	External Stakeholders