PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0045 February 2024

Implementing Biometric Technology at Airports

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Don Zoufal
Kevin Whitney
Erin Manning
Mary Ann Pantle
SDI Presence
Chicago, IL

Robert Boblitz
Baltimore, MD

Richard Duncan
RL Duncan Consulting
Atlanta, GA

Sean Cusson
Del Ray Consulting
Alexandria, VA

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables. The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0045 PROJECT PANEL

Lauren Curtis *Port of Seattle*
Joe Gaudio, Jr. *SSi, Inc.*
Prasanna Kavaipatti *TransSolutions, LLC*
John Delbalso *CHA Consulting, Inc.*
Shawna Larson *City of Phoenix*
Jeremy Martelle *CHA Consulting, Inc.*
Zachary Shuman *Woolpert*
Michael Stubblefield *Safe Skies*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0045 Research Team would like to acknowledge the following organizations and individuals for their contributions to the development of this research. First, National Safe Skies Alliance and Jessica Grizzle for facilitating the research and providing guidance. Second, the PARAS 0045 Project Panel members, who provided significant review and thoughtful comments. And finally, the Research Team would like to thank the various aviation professionals from airports and air carriers, technology service vendors, and federal, state, and local government personnel who generously gave of their time and knowledge to help us prepare this work. Without cooperation and assistance from these experts in their respective fields, completing PARAS research would be much more difficult and the result would not be as rich. We are withholding acknowledgment of individuals and their organizations to protect the confidentiality of the interviews.

CONTENTS

TABLES & FIGURES

SUMMARY

Biometric solutions are being considered by airports to enhance airport access control systems for aviation workers, and at critical processing points in the passenger journey, such as bag drop, security checkpoint passenger screening, and boarding gates. The research in this report provides comprehensive guidance to assist airports and airport stakeholders.

With respect to access control, this report offers general information and case studies on industry deployments. The case studies address issues such as needs assessments, training, privacy concerns, and the deployment of biometrics into the larger context of access control systems.

Regarding the passenger journey, the biometric modality is largely fixed on the facial biometric, which is attributable to the federal agencies managing security operations in connection with domestic and international travel. This report focuses on the evaluation of airport and airline experiences in harmonizing their current practices in passenger processing with federal security requirements for utilizing biometric processes. This analysis applies to multiple processes, including bag drop, security screening, and boarding operations. It also assesses the impacts of those deployments on airport facilities and operations.

A summary of each section of this report is provided below:

Section 1 introduces the general factors driving the expansion of biometric solutions, outlines the methodology employed in this research, and provides an overview of the case studies in Appendices A and B.

Section 2 provides an overview of biometric technology. It explores biometric modalities with emphasis on those in use at airports, and defines the types of authentication. It also summarizes performance and suitability metrics and evaluation resources, discusses challenges with user acceptance, and outlines some concerns about bias in biometric technologies.

Section 3 contains findings on the adoption of biometrics in the airport access control and passenger journey applications. It discusses Customs and Border Protection (CBP) and TSA programs and airline efforts, as well as Government Accountability Office recommendations.

Section 4 focuses on considerations for implementing biometrics in access control applications, including assessing needs and requirements, selecting and reviewing systems, procuring and deploying systems, and addressing legal concerns.

Section 5 focuses on considerations for implementing biometrics in passenger journey applications, including assessing needs and requirements, selecting systems, integrating and deploying systems, and addressing legal concerns.

Section 6 includes a comprehensive review of legal and policy protections in connection with the collection and use of biometric data. The analysis offers airports a detailed understanding of the legal issues that have caused many airports to delay implementation of biometric programs.

Section 7 summarizes considerations for biometric implementation.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

1:1	One-to-One
1:N	One-to-Many
ABG	Automated Biometric Gate
ACRP LRD 42	ACRP Legal Research Digest 42
ACS	Access Control System
ADA	Americans with Disabilities Act
ASSIST	Airport Security Systems Integrated Support Testing
BHS	Baggage Handling System
BIPA	Illinois Biometric Information Privacy Act
CAT	Credential Authentication Technology
CAT 2	Credential Authentication Technology version 2
CAT I	Category I Airport
CAT II	Category II Airport
CAT III	Category III Airport
CAT X	Category X Airport
CATSA	Canadian Air Transportation Authority
CBP	Customs and Border Protection
CHRC	Criminal History Records Check
CHRI	Criminal History Record Information
CIN	CATSA Identification Number
CJIS	Criminal Justice Information Services
DCS	Departure Control System
DoJ	Department of Justice
FAR	False Acceptance Rate
FATE	Face Analysis Technology Evaluation

FIPP	Fair Information Practice Principles
FRR	False Rejection Rate
FRTE	Face Recognition Technology Evaluation
FRVT	Facial Recognition Vendor Tests
FTC	Federal Trade Commission
GAO	Government Accountability Office
IASS	Integrated Airport Security System
ID	Identification
IDMS	Identity Management System
IEEE	Institute of Electrical and Electronics Engineers
IREX	Iris Exchange
MINEX	Minutiae Interoperability Exchange
MINEX III	Minutiae Interoperability Exchange continuing test
MSC	Midfield Satellite Concourse
MSP	Minneapolis/St. Paul International Airport
NCSL	National Conference of State Legislatures
NGO	Next Generation Identification
NIST	National Institute of Science and Technology
PACS	Physical Access Control System
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
POST	Performance and Operational System Testing
PRN	Passenger Record Number
RAIC	Restricted Area Identity Card

TSO	Transportation Security Officer
TVS	Traveler Verification Service
UID	Unique Identifier
US	United States
US VISIT	US Visitor and Immigrant Status Indicator Technology

SECTION 1: INTRODUCTION

Increased airport interest in biometric solutions can be partially attributed to the threats airports face and the increasing suitability of biometrics to support programs designed to address those threats. Commercial use of biometric solutions has increased the public's acceptance of these types of measures, and has made biometric solutions more efficient and cost effective.

Biometric technology holds great promise to optimize the security of access control systems and passenger processing systems. The TSA *Identity Management Roadmap* advocates for use of biometrics to enhance verification processes for both passengers and non-passengers as part of an overall risk reduction strategy.[1] The use of biometrics offers many opportunities for airports, including:

Enhanced Security: Biometric access control offers a higher level of security compared to access cards or personal identification numbers (PIN). Biometric authentication mitigates the risk of unauthorized access to secure areas.

Improved Efficiency: Biometric systems can streamline employee and passenger processing, reducing wait times and moving people more efficiently throughout the airport. Faster and more accurate authentication can lead to improved operational efficiency and passenger satisfaction.

Seamless Passenger Experience: Biometric technology provides a seamless and convenient experience for passengers, eliminating the need to present physical documents repeatedly. It simplifies the passenger journey, reducing friction and enhancing overall satisfaction.

Fraud Prevention: Biometrics can significantly reduce identity fraud and document forgery at airports. By verifying an individual's unique biometric characteristics, it becomes much harder for impostors to gain access or use fraudulent identification documents.

Interoperability and Standardization: Deploying biometric systems at airports provides an opportunity for standardization and interoperability across airports and travel providers. This can lead to smoother travel experiences and improved collaboration among stakeholders.

Data Analytics and Insights: Biometric data can be utilized for analytics purposes. By analyzing passenger and employee flow patterns and behavior, airports can gain valuable insights to optimize operations, security measures, and resource allocations. However, this use of biometric data would have to be clearly communicated to enrollees.

Future Potential: Biometric technology is continually evolving. Advancements will provide opportunities for further improving security, accuracy, and passenger experience in the future.

However, the implementation of biometrics also presents challenges for both access control and passenger journey applications, including:

Scalability: Implementing biometric access control at airports potentially requires handling large worker and/or passenger volumes efficiently. Scaling the system to accommodate peak conditions and future growth can be challenging.

[1] Transportation Security Administration 2022. "TSA Identity Management Roadmap," Washington D.C. at p. 24. Cited at https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf.

Integration Complexity: Ensuring seamless interoperability among various systems is crucial for a smooth deployment. Integrating biometric systems with existing airport infrastructure, such as access control, security, and CBP systems, can be challenging.

False Acceptance/Rejection Rates: Biometric systems may encounter false acceptances, where illegitimate individuals are recognized, and false rejections, where legitimate individuals are not recognized. Minimizing these rates and improving accuracy is important to prevent security vulnerabilities and user inconvenience.

System Reliability: Biometric systems need to be highly reliable and available to ensure uninterrupted service. System failures or technical glitches can cause delays and disrupt stakeholders' operations.

Privacy Concerns: The collection and storage of biometric data raise privacy concerns for enrollees. Striking the right balance between security and privacy while ensuring compliance with relevant regulations can be challenging.

1.1 Research Methodology

Extensive literature has been developed concerning biometrics, and there are several different programs that have sought to apply biometric solutions in the aviation context. A 2021 ACRP study titled *Airport Biometrics, a Primer*[2] offers a solid platform for PARAS 0045. That research includes a literature review and several case studies of aviation sector efforts to put biometric processes into practice. The limiting element for the ACRP biometric analysis is that it contains little scrutiny of airport use of biometrics in the physical access control system (PACS) context. With respect to PACS applications, guidance is provided in the RTCA DO–230-K: *Standards for Airport Security Access Control Systems*.[3]

The research for the guidance developed under PARAS 0045 sought to update and fill the gaps in the previous research. This effort applied a mixed-method approach that included:

- Review of original source documents, including governmental reports and policy documents, procurement-related documents, legislation, and court opinions
- Comparative policy analysis
- Brief survey questions administered at conferences and meetings to elicit data on biometric use and biometric modalities
- Structured interviews of airport and airline professionals engaged in biometrics projects
- Onsite visits to examine biometric deployments
- Case study analyses of biometric deployments

1.2 Case Studies

The case studies conducted for this research demonstrate that the totality of the airport's access control systems and its badging and enrollment practices are important considerations. The implementation of biometrics requires integration into a large and complex system governing access. Accordingly, choices of biometric modalities and the way they are employed are often constrained by larger system requirements or limitations.

[2] National Academies of Sciences, Engineering, and Medicine. 2021. *Airport Biometrics: A Primer*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26180.
[3] RTCA Paper No. 079-21/SC224-156, published June 17, 2021.

Table 1 summarizes the biometric access control systems deployed at the airports that were included in the case studies for this project. This table also includes each airport's future biometric considerations. Note that not all airports with existing biometric deployments were considering additional biometric deployments in the future.

Table 1. Research Data on Biometric Access Control Deployments

AIRPORT	TODAY	FUTURE
Category	Biometrics Currently Using for Access Control	Biometrics Exploring for Access Control
X	Fingerprint	—
X	Fingerprint	Fingerprint, Iris, Facial, Other
X	—	—
X	Fingerprint, Facial	Fingerprint, Facial
X	Fingerprint	Iris, Facial
X	—	—
X	Fingerprint	Iris, Facial
X	Iris	Fingerprint, Iris, Facial
X	—	Fingerprint, Iris, Facial
X	Fingerprint	Iris, Facial
X	Facial	Fingerprint
X	Fingerprint, Facial	Fingerprint, Iris, Facial, Other
X	Facial	Fingerprint, Facial
I	Facial	Fingerprint
I	—	—
I	—	Iris, Facial
I	Fingerprint	—
I	—	Fingerprint, Iris, Facial
I	—	—
I	Facial	Fingerprint
I	—	—
II	—	—
II	—	—
II	Fingerprint	Iris, Facial
II	Fingerprint	Fingerprint
II	Fingerprint	—
II	—	Fingerprint
III	—	Fingerprint
III	—	—
Canada	Fingerprint, Iris	—

Each of the case studies in the appendices details lessons learned with respect to the specific biometric application and purpose. Appendix A covers access control applications and Appendix B includes passenger journey applications. For airports interested in a particular biometric and/or process, the relevant case study should be consulted.

A1: Fingerprint Biometric for Access Control – This case study reviews two large airports that have had fingerprint biometric programs for over ten years and utilize similar biometric reader and access control technologies.

A2: Facial & Fingerprint Biometric for Access Control – This case study reviews a large airport that operates two biometric modalities in their access control system. The airport introduced fingerprint biometric access control in 2006 and added a facial biometric system in 2018.

A3: Facial Biometric Pilot for Vehicle Access – This case study discusses a biometric vehicle access control program intended to process vehicles at speed at midfield access checkpoints to reduce current queuing issues.

A4: Facial Biometric Pilot for Access Control – This case study describes the airport's pilot program to add facial biometric for access control. The airport previously used hand geometry biometric devices but discontinued their used during the COVID-19 pandemic.

A5: Fingerprint Biometric for Access Control (Two Airport System) – This case study describes two airports that were among the first in the US to deploy biometrics in an operational setting. Both airports use separate instances of the same biometric/access control/credentialing system.

A6: Iris/Fingerprint Biometric for Access Control (Canada) – This case study describes the centralized biometric access control program deployed at Canadian airports. While the centralized nature of the system has no current applicability to US airports, the lessons of its use of both fingerprint and iris biometrics can be helpful to airports considering those technologies.

B1: Curb-to-Gate Solution Pilot – This case study describes a major airline's introduction of a Curb-to-Gate biometric passenger journey to an airport after testing the concept at other US airports. The airline led the implementation team in coordination with TSA, CBP, and airport stakeholders.

B2: Biometric Bag Drop – This case study reviews biometric bag drop processes operated by two major airlines at one airport. The two projects had significantly different levels of airport involvement.

B3: Biometric Common-Use E-Gate – This case study details an airport's efforts to develop common-use, an automated biometric gate solution, with a focus on improving the passenger processing experience, enhancing security, and increasing operational efficiency. The airport's approach recognized that the integration of multiple air carriers into a single, common-use platform necessitated a flexible solution capable of meeting each carrier's needs.

SECTION 2: BIOMETRIC TECHNOLOGY OVERVIEW

Conventional access control systems often use single-factor authentication based on something a person has in their possession, such as a card. To increase security, a second factor can be added, e.g., something they know, like a PIN. But since cards can be lost, stolen, or loaned to another person to gain access, and PINs can be forgotten, guessed, or observed by others, biometrics are now being considered by airports wanting additional security assurance. With biometrics, there is a confirmed link to an actual person rather than a lost or stolen item. A biometric feature is also more difficult to copy or steal than a PIN.

Each biometric modality and product has unique properties that can affect its performance, such as usability and human factors. For example, the biometric sensor should be readily accessible to individuals at various heights, including those who are seated in a wheelchair. Consideration should also be given to individuals who may not be able to present a biometric sample due to injury or other physical disability. Use of multimodal biometrics, such as fingerprint and iris, can provide flexibility to address this type of situation. Another alternative is to allow use of a PIN in lieu of biometrics for only those individuals who cannot submit a usable biometric sample.

Even within the same biometric modality, different vendor products can yield different levels of performance. Performance metrics or characteristics that should be considered are discussed in Section 2.3. Procedures for handling operational issues should also be given careful consideration.

There are various biometric modalities that can be utilized for identification. The characteristics of those modalities make some biometrics more effective and efficient for commercial use. This section presents an introduction to biometric modalities and offers some methods of comparing different modalities for various uses.

2.1 Modalities in Use at Airports

There are numerous biometric tools for identifying individuals; some of the more common ones are:

- Fingerprint Recognition
- Facial Recognition
- Iris Recognition
- Hand Geometry Recognition
- Vascular Pattern Recognition

Hand geometry has been utilized in at least one airport, but was discontinued and replaced with a fingerprint biometric due to the size of the hand geometry readers and superior performance of fingerprint biometric. Accordingly, hand geometry was not evaluated in depth for this report. Airports have now focused on technologies using fingerprint, facial, and iris biometric modalities.

Fingerprint recognition uses the physical structure of an individual's fingerprint. Important features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings.[4] The fingerprint biometric is the most commonly used modality in US airports in connection with access control. Typically, these solutions are deployed at specific portals, such as those connecting public areas

[4] Radio Technical Commission for Aeronautics, DO-230L Standards for Airport Security Access Control Systems, December 15, 2022. https://my.rtca.org/productdetails?id=a1BDm000000GuyNMAS.

to Sterile or Secured Areas or Sterile Areas to Secured Areas. At one CAT X airport, access to the Sterile Area from the passenger screening checkpoint is controlled through fingerprint biometrics.

Facial recognition uses an image of the visible physical structure of an individual’s face. Both two dimensional and three-dimensional facial recognition technologies can be used. Today, advanced facial recognition algorithms are based on deep neural networks or “machine learning” technology.[3]

Iris recognition uses an image of the physical structure of an individual’s iris. The iris muscle is the colored portion of the eye surrounding the pupil and is acquired using near-infrared illumination from a distance of at least twelve inches. It should be noted that iris recognition is often confused with retinal scanning, which is a scan of the blood vessel pattern in the back of the eye using a close-proximity and high-intensity light source. Because of usability issues, retinal scanning is not a commercially available biometric method.[3]

As of 2023, only one CAT X airport is known to have initiated a system-wide facial biometric access control deployment. Several other airports have had test deployments of facial recognition, and some are interested in adding facial biometric enhancements or other biometrics to their access control systems, indicating a growing interest in this technology within the airport industry.

Among US airports prior to 2023, only one CAT X airport reported employing facial biometrics for access control. However, this application is limited to a small number of portals within the airport. They continue to also utilize fingerprint access control at those portals and several others. The fingerprint and facial recognition biometrics operate independently at the portals where they are both deployed. Both the fingerprint and facial biometrics are encoded in the access credentials of authorized individuals only.

The use of iris biometrics for access control is common in Canadian airports. In 2007, the Canadian Air Transportation Security Authority (CATSA) began implementing a Restricted Area Identity Card (RAIC) program. It provides for an access control system using iris and fingerprint identifiers in conjunction with chip-enabled smart cards for access control at the twenty-nine highest-security airports.

2.2 Authentication Types

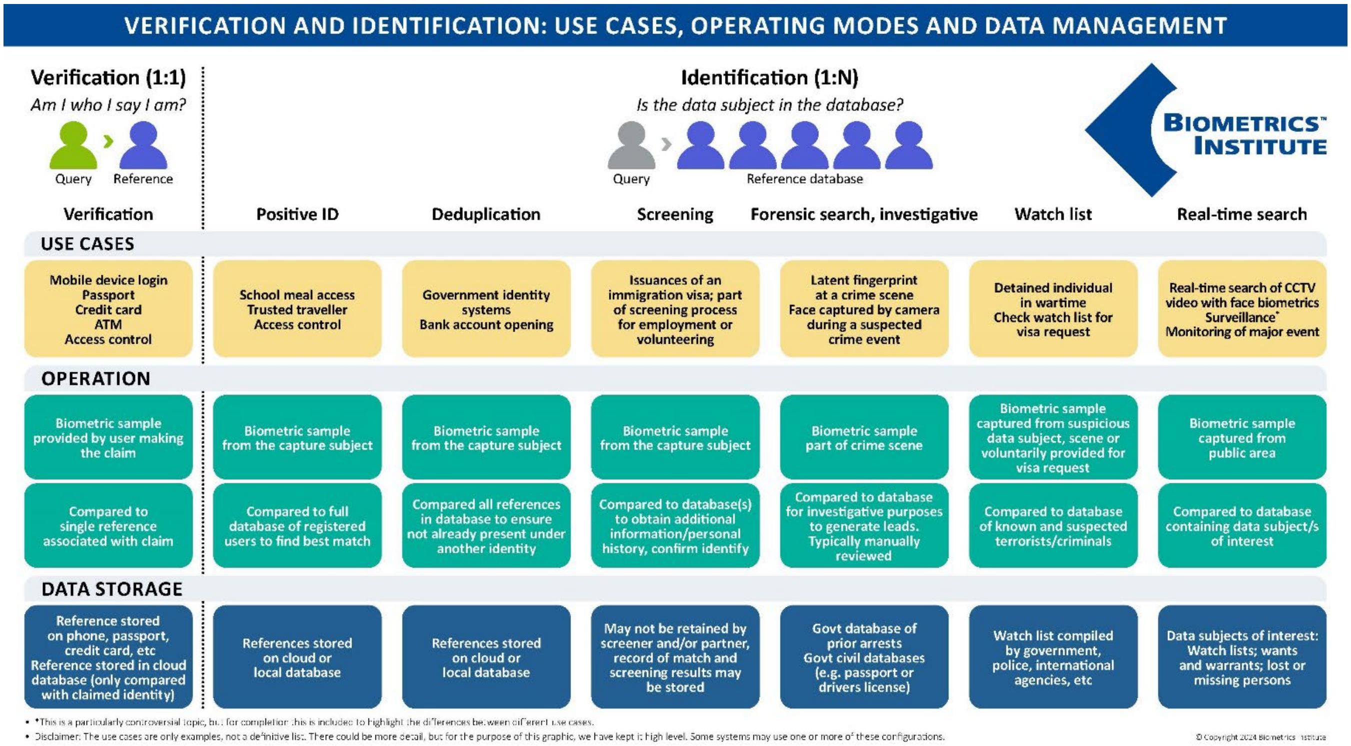
Biometric authentication is performed by comparing a biometric presented at the reader to a biometric template stored for the individual. This can be processed as either a one-to-many (1:N) or one-to-one (1:1) comparison, depending on the system setup.

In 1:N processes, the system analyzes the user’s biometric against a database of all enrolled templates or a subset thereof (also known as one-to-few). This type of process is used to identify a person from a database without the use of a badge or travel document.

In 1:1 processes, authentication is performed by comparing the presented biometric to a single template stored either on a smart card or in a central database. This process requires the user to present a identification item (i.e., a badge, smart card, or other physical ID) which accesses the specific template that is used in the biometric transaction.

Figure 1 shows each authentication type’s use cases and operating and data storage modes.

Figure 1. Comparison of 1:1 and 1:N Authentication Types



VERIFICATION AND IDENTIFICATION: USE CASES, OPERATING MODES AND DATA MANAGEMENT

Verification (1:1)

Am I who I say I am?

Identification (1:N)

Is the data subject in the database?

Query
Reference
Query
Reference database
BIOMETRICS INSTITUTE

	Verification	Positive ID	Deduplication	Screening	Forensic search, investigative	Watch list	Real-time search
USE CASES	Mobile device login Passport Credit card ATM Access control	School meal access Trusted traveller Access control	Government identity systems Bank account opening	Issuances of an immigration visa; part of screening process for employment or volunteering	Latent fingerprint at a crime scene Face captured by camera during a suspected crime event	Detained individual in wartime Check watch list for visa request	Real-time search of CCTV video with face biometrics Surveillance* Monitoring of major event
OPERATION	Biometric sample provided by user making the claim	Biometric sample from the capture subject	Biometric sample from the capture subject	Biometric sample from the capture subject	Biometric sample part of crime scene	Biometric sample captured from suspicious data subject, scene or voluntarily provided for visa request	Biometric sample captured from public area
	Compared to single reference associated with claim	Compared to full database of registered users to find best match	Compared all references in database to ensure not already present under another identity	Compared to database(s) to obtain additional information/personal history, confirm identify	Compared to database for investigative purposes to generate leads. Typically manually reviewed	Compared to database of known and suspected terrorists/criminals	Compared to database containing data subject/s of interest
DATA STORAGE	Reference stored on phone, passport, credit card, etc Reference stored in cloud database (only compared with claimed identity)	References stored on cloud or local database	References stored on cloud or local database	May not be retained by screener and/or partner, record of match and screening results may be stored	Govt database of prior arrests Govt civil databases (e.g. passport or drivers license)	Watch list compiled by government, police, international agencies, etc	Data subjects of interest: Watch lists; wants and warrants; lost or missing persons

- *This is a particularly controversial topic, but for completion this is included to highlight the differences between different use cases.
- Disclaimer: The use cases are only examples, not a definitive list. There could be more detail, but for the purpose of this graphic, we have kept it high level. Some systems may use one or more of these configurations.

Source: Biometrics Institute

2.3 Performance and Suitability Metrics

Biometric modalities can be assessed on the following elements:

- Maturity – This refers to how long a modality has been in use. More mature modalities can offer detailed performance histories and have addressed initial issues.
- Accuracy – This is the key performance indicator of the modality's ability to acquire and "match a biometric sample at a level of accuracy that meets the requirements of the intended application."[3] The following measurements are used to express a biometric system's accuracy:
    - False Rejection Rate (FRR) – the frequency that a biometric system fails to accept (match) the authorized individual to their enrolled biometric template.
    - False Acceptance Rate (FAR) – the frequency that a biometric system incorrectly accepts (matches) an unauthorized individual's presented biometric to a different individual's enrolled biometric template.
    - Equal Error Rate – the point at which the FRR and FAR lines intersect, and the percentage of false acceptances and false rejections are the same.
    - Failure to Enroll Rate – the rate at which individuals cannot be enrolled into a system because they cannot present a biometric sample meeting the required system thresholds.
    - Failure to Acquire – a system's failure to extract usable data from a biometric sample after successful enrollment in the system.
- Template Size – Each biometric template is a set of stored features collected from an individual and stored in a database or on a card. Template size varies based on the biometric modality.

- Cost – The Total Cost of Ownership of a system. This incorporates the entire life cycle cost of the system, including implementation, enrollment, field devices, badge media, data security, adaptability, and maintenance.
- Security – Along with the duplication risk noted below, this refers to the biometric's uniqueness to an individual and its FAR.
- Duplication Risk – Along with security noted above, this refers to the likelihood the biometric can be duplicated to allow someone to 'fake' the biometric and achieve a false acceptance.
- Long Term Stability – The permanence, availability, and reliability of the biometric both in terms of the individual's physical biometric and the stored template captured.
- Processing Speed – The time required to present, capture, and match the biometric sample. The time that it takes to process and match a biometric sample will depend on several variables. It is typically faster to perform a verification (1:1 comparison) biometric match than to search an entire population of registered users to perform a biometric match (1:N comparison).[4]
- Ease of Use – How easy the biometric system is to use for the individual, including Americans with Disabilities Act (ADA) considerations. This also ties to environment where some biometrics can be more challenging to use in one environment over another. For example, fingerprints are easier to use in a warm outdoor climate versus a colder climate where users wear gloves.
- Intrusiveness – Refers to whether an individual must physically contact the device. This can also refer to the enrollment process. For example, retinal enrollment requires a high-intensity light to shine to the back of the eye, which is intrusive, while iris enrollment uses a camera to capture the iris pattern.
- Environment Adaptability – Operating environmentals factors like temperature, humidity, dust, and lighting can potentially impact the biometric system. In some cases, a system could potentially be adapted to perform well in an otherwise challenging environment (e.g., installing a cover to minimize dust on a fingerprint biometric reader). The users' work type may also impact performance. For example, an iris biometric system may not be ideal for a population that must wear protective glasses.

In recent years, there has been a notable improvement in the availability, accuracy, and efficiency of biometric access control solutions, particularly those utilizing facial recognition technology. However, despite the wide range of products available, very few have been implemented or tested specifically in the aviation market. To comprehensively evaluate the functionality of these technologies, they must be integrated with other systems such as access control systems, identity management systems, and access card media.

Piloting and testing biometric products can be costly and may create procurement challenges for airports. However, Safe Skies' ASSIST program offers the opportunity for airports to pilot biometric access control technology projects, allowing them to assess the effectiveness and feasibility of different solutions.

To aid in the evaluation of biometric solutions, the National Institute of Standards and Technology (NIST) has also developed tools and ongoing evaluation programs that help assess the performance and interoperability of various biometric products. The NIST website is regularly updated to reflect advancements in technology, and it serves as a valuable source for staying informed about new biometric solutions.

- NIST: https://www.nist.gov/programs-projects/biometrics
- Fingerprint solutions: https://www.nist.gov/programs-projects/fingerprint
    - The Minutiae Interoperability Exchange (MINEX) with its ongoing MINEX III evaluation program: https://www.nist.gov/itl/iad/image-group/minutiae-interoperability-exchange-minex-iii)
- Facial solutions: https://www.nist.gov/programs-projects/face-projects
    - Face Recognition Vendor Tests (FRVT) evaluates the performance of a range of products including the FRVT 1:1 Verification https://pages.nist.gov/frvt/html/frvt11.html
- Iris Solutions: https://www.nist.gov/programs-projects/iris-exchange-irex-overview
    - The IREX 10 is a platform for ongoing testing of iris biometric solutions https://pages.nist.gov/IREX10/

Additionally, DHS has organized several rallies to facilitate the testing of biometric solutions, further promoting innovation and development in the field.

Overall, the growth of the biometric market offers numerous options, but the evaluation and integration of these solutions within the airport environment require careful consideration of various factors. Collaboration with industry programs, such as ASSIST, and utilizing resources, like those provided by NIST, can help airports make informed decisions and select effective biometric access control technologies.

2.4 User Acceptance

Surveys published by the University of Texas in 2018 and the Institute of Electrical and Electronics Engineers (IEEE) in 2022 examined the attitudes of US adults toward biometric use.[5, 6] The biometrics studied included fingerprint, facial recognition, hand geometry, iris scan, voice recognition, and DNA. Results indicated that most adults were most comfortable with the fingerprint biometric; users' comfort levels with other biometrics were mixed.

The 2022 IEEE paper noted a correlation between an individual's experience using a particular biometric and the expressed comfort with use. It was unclear whether comfort was attributable to the use experience or if the use experience was a function of the comfort level. The research also raised questions over whether the comfort level was affected by perceptions of the difficulty of enrollment. Both studies noted that comfort level and confidence were affected by the context in which the biometric modalities were being used.

For example, the IEEE study noted most people surveyed indicated being comfortable using either fingerprint or facial recognition biometrics with respect to accessing devices like smartphones. However, the majority of survey respondents indicated they were not comfortable with the use of biometrics in connection with activities like tracking movements of retail shoppers within a store to offer them discounts, or a coffee shop using biometrics to register and track customers in their loyalty

[5] German, Rachel L, and K Suzanne Barber. Rep. *Consumer Attitudes About Biometric Authentication*. The University of Texas at Austin, Center for Identity, May 2018. https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf.

[6] Katsanis, Sara H, Peter Claes, Megan Doerr, Robert Cook-Deegan, Jessica D Tenenbaum, Barbara J Evans, Life Senior Member, IEEE, et al. Publication. *U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics* 3. 1st ed. Vol. 3. Accessed February 2024. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9576819.

programs. The research did not note any appreciable difference in response about comfort levels based on demographic differences.

The results of these surveys suggest that familiarity with the biometric modality selected will influence acceptance and adoption. In that regard, fingerprint biometrics will likely have an advantage with respect to aviation worker comfort levels since they already undergo fingerprinting in the credentialing process. As for facial biometrics, its growing use as a security measure for device access, as well as its adoption in connection with passenger journey solutions and new identity programs like mobile driver's licenses will also likely serve to enhance comfort levels.

Conversely, given their comparatively infrequent use, it is likely that users will be the least comfortable with iris biometric systems.

2.5 Concerns About Bias

Understanding and mitigating bias in the use of facial biometrics is an important consideration. Many of the movements to limit or prohibit the use of biometrics are related to concerns about bias in the algorithms that support the applications. A 2018 Massachusetts Institute of Technology Media Lab study raised significant concerns with its conclusions that some facial recognition systems produced error rates of up to 34.7% in persons other than white males.[7]

In response to these concerns, NIST conducted a test of facial recognition algorithms to assess the issue of bias, among other factors. In December 2019, NIST issued a report on the subject of bias (the NIST Bias Report)[8] that validated some concerns about biases in the algorithms that power facial recognition solutions. It noted that facial recognition solutions varied with respect to the effect bias had on accuracy in certain demographic groups. In some cases, the differences in accuracy were significant.

The importance of addressing potential bias in facial biometric solutions is outlined by the GAO in its report evaluating facial recognition solutions employed by CBP and TSA.[9] The GAO made the following evaluation regarding the algorithm utilized by CBP:[10]

> A recent NIST evaluation in December 2019 focused on testing the effects of demographics on matching accuracy of over 100 commercially available facial recognition algorithms. [footnote omitted]. NIST found that demographic effects in matching accuracy varied significantly across the algorithms it tested and that many facial recognition systems performed differently among demographic groups. While NIST did not evaluate TVS, it included a version of the algorithm CBP uses with TVS in its evaluation and found it was among the most accurate algorithms on many measures.

The GAO observed that the issue of bias was specific to the algorithms. Some algorithms in the NIST Bias Report demonstrated consistency across racial and ethnic groups. Since the 2019 NIST report, there

[7] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1-15, Conference on Fairness, Accountability & Transparency (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[8] National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (Gaithersburg, MD: 2019). Cited at https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

[9] General Accountability Office 2020. "Facial Recognition, CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues" GAO Report 20-568 (September 2020) P.14 and Appendix I. Cited at https://www.gao.gov/assets/gao-20-568.pdf.

[10] Id at P.14.

have been significant efforts by facial recognition vendors to remove bias, and much progress has been made.

The important lesson for airport operators is the need to evaluate and understand the biases that may be present in algorithms that support facial recognition solutions they are considering. NIST is conducting ongoing studies of facial biometric technologies, including the Face Recognition Technology Evaluation (FRTE) and the Face Analysis Technology Evaluation (FATE), in which over 100 commercial algorithms for facial recognition have been tested. The results are available on the NIST website.[11] Airport operators should consider consulting the NIST testing in conjunction with the selection of facial recognition solutions, and perhaps even set procurement standards based on NIST's findings.

[11] **NIST FRTE/FATE Studies:** https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate.

SECTION 3: CURRENT AIRPORT BIOMETRIC USE

The decision to introduce biometrics into airport processes, whether for aviation operations or passengers, presents numerous considerations, including the following:

- **Security enhancement:** the nature of the threats and the value that biometric identification adds in addressing the threats
- **Operational efficiency:** understanding the impact of adding complexity to existing processes, effects of throughput, ability to deploy across operating conditions, additional process requirements such as enrollment, and infrastructure capacity to integrate with existing processes
- **User acceptance:** the perceptions, preferences, and willingness of aviation workers and passengers to adopt and follow new biometric processes
- **Regulatory and compliance:** ensuring that biometric deployments meet government regulatory requirements
- **Reputational issues:** the perception that the airport is taking reasonable measures to address legitimate security concerns and maintain efficient operations.
- **Privacy and civil liberties:** ensuring that the airport and airlines respect the sensitive nature of biometrics and related personally identifiable information (PII).

The introduction of biometrics is being driven by several currents in the aviation industry, including:

- Pandemic-driven desire to implement touchless solutions for aviation workers and passengers
- Increased spotlight on addressing insider threats
- Growing availability of accurate biometric systems at lower costs
- Labor savings resulting from introducing more efficient operating systems for passenger and aviation worker processing
- Increased user familiarity and confidence in biometric technologies

One of the principal impediments to the adoption of biometric technologies is concern over potential legal restrictions on biometric use.

3.1 Current State of Biometric Access Control

Government and the aviation industry both recognize the persistent danger of insider threats. The TSA's *Insider Threat Roadmap 2020* chronicles the ways in which authorized access has been used over the last decade to conduct criminal activity.[12] The importance of enhanced access control, including controls using biometric technologies, was noted in a 2020 GAO study of airport security measures to combat insider threats.[13]

For biometrics in access control, the TSA's approach has been largely advisory in nature. While the federal government has long advocated for enhanced measures to control access to regulated areas of airports, there is no current requirement to implement biometric access control. However, the federal government, through TSA actions like acceptance of biometric access records in lieu of physical audit

[12] Transportation Security Administration 2020. "Insider Threat Roadmap 2020," Washington D.C. at p. 6. Cited at https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

[13] General Accountability Office 2020. "TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals" *GAO 20-275*. Washington D.C. Cited at https://www.gao.gov/assets/gao-20-275.pdf.

requirements for access media, has encouraged the implementation of biometric-based access control systems.

Biometric-based identity verification methods are key pillars in the security of US airports. Conducting fingerprint-based background checks has long served as a cornerstone of credential management. Applying biometric measures to the access control transaction at secured portals and gates is a logical next step that extends identity security to all parts of an airport facility.

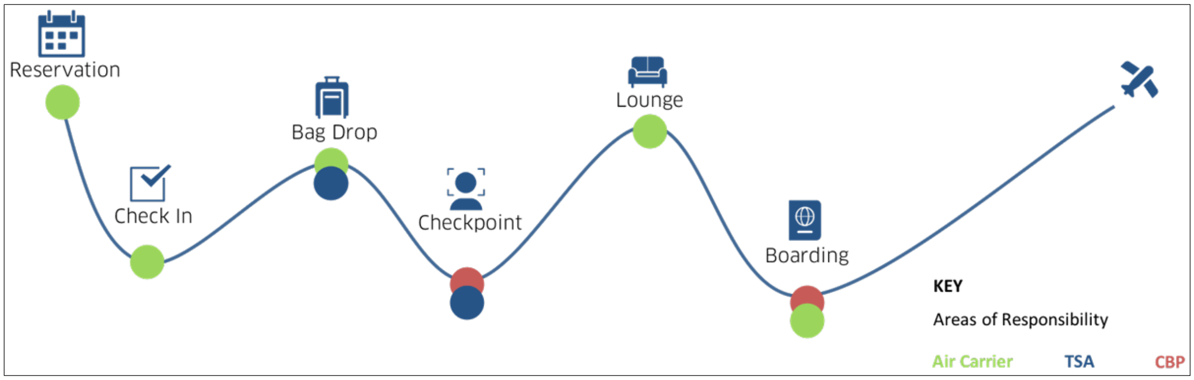
One of the first large-scale biometric access control deployments occurred in 2007 when a US airport implemented biometric access control to Secured and Sterile Areas. Biometric programs have evolved over the years, and an increasing number of airports have begun adopting biometric access programs, mainly using fingerprint biometrics. Canada has adopted iris biometrics along with fingerprints. More recently, developments in the reliability of facial biometrics have increased focus on that modality. The COVID-19 pandemic and the desire to move to touchless access control solutions further increased this focus.

While offering several benefits in terms of speed of access and increased security, adopting biometrics into PACS holds implications for a range of activities in the airport environment. As with the adoption of any new technology, the movement to biometric-based PACS requires executing a range of change management strategies to ensure smooth integration. This includes training in the operation of new biometric technologies at all levels of the airport enterprise, including stakeholder users. Securing stakeholder support is a critical element when transitioning to these new platforms.

3.2 Current State of Biometrics in the Passenger Journey

In addition to reinforcing security requirements with respect to employee access, biometrics has been seen as a measure to improve both the security and efficiency of passenger processing. In 2018, TSA released its *TSA Biometric Roadmap*,[14] which included Figure 2 below, depicting the process and the stakeholders involved.

Figure 2. Notional Biometric Passenger Experience Stakeholder Roles and Responsibilities[15]



Source: TSA Biometric Roadmap

At the forefront of the biometric revolution in airports is the check-in process, where traditional methods involving lengthy queues and manual verification can be replaced by biometric solutions. Biometric kiosks scan a passenger’s face and match it against pre-registered data, allowing for a faster, more

[14] Transportation Security Administration 2018. “TSA Biometric Roadmap, For Aviation Security & the Passenger Experience,” p.18. Cited https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[15] *Id.*

efficient, low contact check-in experience. Further, biometrics can be integrated into self-service bag drop systems, expediting the baggage handling process and reducing human error.

At passenger screening checkpoints, facial recognition systems can authenticate a traveler's live image against their pre-captured identification image.

Biometric applications extend to the boarding gate as well, eliminating the need for physical boarding passes. Facial recognition scanners match passengers against flight manifests, allowing for smooth, efficient, and low- or no-contact boarding processes.

Examples of these processes have already appeared in airports across the US.[16] In June 2017, Delta Air Lines launched a biometrically enabled self-service bag drop at Minneapolis/St. Paul International Airport (MSP).[17] Delta expanded the program in 2018 to include curb-to-gate processing in Atlanta, Salt Lake City, and MSP.[18] In January 2018, Los Angeles International Airport launched biometric e-gates for boarding flights departing the US.[19] Many of those efforts went on hiatus during the pandemic but are now being revived.

The implementation of biometrics to support the passenger journey has resulted in different approaches and programs in airports across the country. The case studies in Appendix B outline some of the different approaches taken to address passenger processing challenges.

The use of biometrics in passenger processing is not entirely new, as the Registered Traveler program has been utilizing biometrics, including iris and fingerprint recognition through the CLEAR program, for over a decade.

As of November 2023, the CLEAR website reports that the CLEAR application is in use at more than 50 airports in 45 cities across the US.[20] This wide implementation demonstrates a growing acceptance and adoption of biometric technology for the passenger journey.

Facial biometric technology has emerged as TSA and CBP's preferred modality for passenger processing, as it offers a convenient and non-contact method of identity verification. Several airports across the country have conducted testing involving facial biometrics at different points of the passenger journey where identity verification or visual confirmation is typically required, such as bag drop, security screening, and boarding. CBP directed much of the boarding gate testing in conjunction with their program for entry and exit monitoring.

According to the CBP website, as of November 2023 CBP's facial recognition program is active at all US international airports for entrance processing and at forty-six airport locations for exit processing, including fifteen CBP Preclearance locations outside the United States.[21, 22] The biometric monitoring

[16] See, e.g., National Academies of Sciences, Engineering, and Medicine 2021. "Airport Biometrics: A Primer." Washington, DC: The National Academies Press. Cited at https://doi.org/10.17226/26180.

[17] Delta Opens First Biometric Self-Service Bag Drop in U.S., (2020), https://news.delta.com/delta-opens-first-biometric-self-service-bag-drop-us.

[18] Delta Airlines. "Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers." News Hub, Delta Official Website. Cited at https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers.

[19] Successful Biometric E-Gate at LAX Blazes Trail for Commercial Aviation, Int'l Airport R. (Jan. 19, 2018), https://www.internationalairportreview.com/news/64154/biometric-e-gate-lax-aviation.

[20] **Clear:** https://www.clearme.com/where-we-are.

[21] **US CBP Biometrics**: https://biometrics.cbp.gov/#.

[22] **US CBP Preclearance:** https://www.cbp.gov/travel/preclearance.

process for foreign nationals entering and exiting the United States is part of a statutorily mandated program implemented under the US Visitor and Immigrant Status Indicator Technology (US VISIT) program in DHS.[23]

Two CAT X airports are piloting complete curb-to-gate biometric solutions. These comprehensive implementations involve significant coordination with federal government partners to integrate with existing security systems.

As of March 2023, biometric bag-drop solutions and the CBP entry and exit process for international boarding seem to be the biometric processes most often deployed for passenger processing at airports.

3.3 CBP & TSA Biometric Processes

Three different programs or initiatives evidence the US federal government's commitment to promoting biometric use in the aviation and travel sector: CBP's Traveler Verification Service (TVS), TSA's credential authentication technology (CAT) pilot programs, and TSA guidance documents concerning biometric enhancement to access control.

CBP and TSA processes pertaining to the passenger journey are internally developed and implemented by these federal agencies. Although they govern the activities of these agencies, these processes may substantially impact air carriers and airports.

To support efforts to integrate the use of biometric technology in the passenger journey, TSA and CBP have been working to develop the TVS,[24] operated by CBP, and CAT,[25] operated by TSA. Both agencies have partnered with US air carriers to test these systems for domestic and international travel.[26]

While these programs are in their early stage of development and are not yet mandatory, the federal government appears to be moving quickly in that direction. In 2018, TSA and CBP signed a policy memorandum to work collaboratively on the development and use of biometric technology at airports. This approach will help to mitigate the possibility of duplicate or inconsistent federal requirements being applied to passenger processing.

3.3.1 CBP Traveler Verification Service

The TVS is the product of an over twenty-year process to develop automated technology to monitor foreign traveler passage into and from the United States in a fashion that is consistent with air carrier operational requirements and airport infrastructure limitations. The Privacy Impact Assessment (PIA) for the TVS summarizes the statutory and regulatory actions taken post-9/11 that charged DHS, and

[23] **US VISIT:** https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_brochure_english.pdf.

[24] U.S. Customs and Border Protection. "Biometric Air Exit Business Requirements," Version 2.0. January 2020 Cited at https://www.cbp.gov/sites/default/files/assets/documents/2020-Jul/Exit%20BRD2__Redacted_0.pdf.

[25] Transportation Security Administration, "Travel Document Checker Automation-Digital Identity Technology Pilots" Privacy Impact Assessment DHS/TSA/PIA 51 (January 14, 2022). Cited at https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-tsa051-digitalidentitytechnologypilots-january2022_0.pdf.

[26] Marcy Mason, "Biometric Breakthrough" Frontline Magazine (September 28, 2022) Cited at https://www.cbp.gov/frontline/cbp-biometric-testing.

ultimately CBP, with developing a program to monitor the exit and entry of foreign nationals in the US.[27]

The capture of biometric data for entering individuals commenced under the US-VISIT program in 2004.[28] In 2016, CBP initiated a pilot to test facial recognition technology for exit monitoring applications. Based on the results of the pilot testing, CBP developed the TVS in 2017 to institute facial matching biometrics in support of their operations.[29] It has rolled out initially in the air travel environment with plans to expand it to all ports of entry.

The TVS program matches live images of individuals against a database of photographs drawn from passports and other travel documents, as well as from entry inspections or other DHS encounters. The TVS uses two matching processes:

- In cases where CBP receives passenger manifests, a gallery of passenger photos from its database is prepared and the system conducts a 1:N comparison of the live photo of the traveler against the gallery of photos.
- Where a manifest is unavailable, the TVS can conduct 1:1 matching of a photo of the traveler against a photo in a travel document.

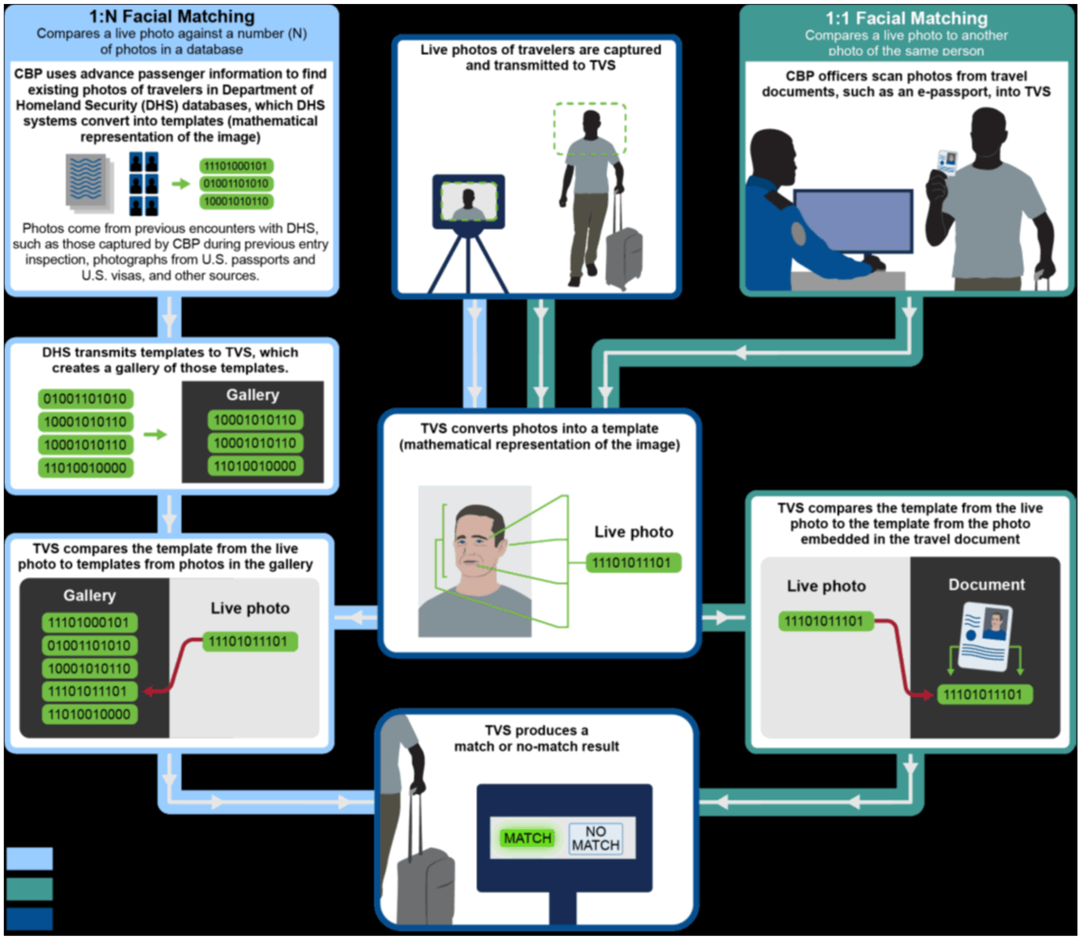
Figure 3 shows how the process works in each instance.

[27] U.S. Customs and Border Protection. "Privacy Impact Assessment for the Travel Verification Service" DHS/CBP/PIA-056. (November 18, 2018). Cited at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[28] U.S. Department of Homeland Security. US-VISIT Program, Increment 2 Privacy Impact Assessment" (September 14, 2004). Cited at https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf.

[29] U.S. Customs and Border Protection. "Privacy Impact Assessment for the Travel Verification Service" DHS/CBP/PIA-056. (November 18, 2018). Cited at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

Figure 3. TVS Facial Matching System


1:N Facial Matching
Compares a live photo against a number (N) of photos in a database
CBP uses advance passenger information to find existing photos of travelers in Department of Homeland Security (DHS) databases, which DHS systems convert into templates (mathematical representation of the image)
11101000101
01001101010
10001010110
Photos come from previous encounters with DHS, such as those captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and other sources.
Live photos of travelers are captured and transmitted to TVS
1:1 Facial Matching
Compares a live photo to another photo of the same person
CBP officers scan photos from travel documents, such as an e-passport, into TVS
DHS transmits templates to TVS, which creates a gallery of those templates.
01001101010
10001010110
10001010110
11010010000
Gallery
10001010110
10001010110
11010010000
TVS converts photos into a template (mathematical representation of the image)
Live photo
11101011101
TVS compares the template from the live photo to templates from photos in the gallery
Gallery
11101000101
01001101010
10001010110
11101011101
11010010000
Live photo
11101011101
TVS compares the template from the live photo to the template from the photo embedded in the travel document
Live photo
11101011101
Document
11101011101
TVS produces a match or no-match result
MATCH
NO MATCH

Source: GAO-20-568

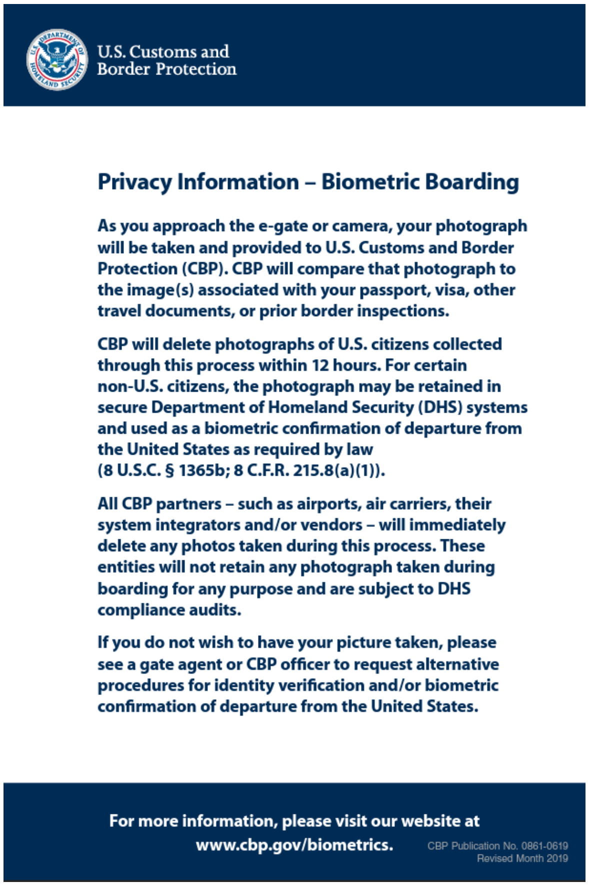
Entry screening processes takes place entirely in the FIS area of an airport, while exit screening can occur at multiple departure areas of the airport, which can include multiple terminals and gate areas. Accordingly, CBP exit screening activity needs to be coordinated with airports and airlines so that equipment and personnel can be present to conduct the screening.

CBP's process for screening exiting passengers works in conjunction with airline partners at departure gates. Those airlines must agree to the TVS business requirements, which lay out the process for transfer of the biometric data, and prohibit the airlines from retaining the biometric information. Technical processes must be coordinated between CBP and the airline and/or airport, depending on who is collecting the biometric data.

Airline and airport cooperation with the collection and transmission of biometric data is currently voluntary. As noted above, departure screening does not compel biometric checks of US citizens or some categories of foreign nationals. While the implementation of automated biometric systems greatly facilitates CBP's efforts to achieve their mandate for biometric monitoring of exiting foreign nationals, neither airports nor air carriers are required to install technology to aid CBP compliance with congressional requirements. Therefore, CBP is incentivizing the rollout of automated solutions by advising airports and air carriers that if compliance with the exit monitoring mandates is not achieved through the automated systems, CBP resources will need to be diverted from other airport functions to meet the mandates. To that end, CBP has begun a robust monitoring program to measure achievement of exit monitoring goals. CBP has been preparing monthly reports regarding the adoption of biometric screening for outbound passengers. These reports reflect forty-seven participating airports. In April 2023, a little over a quarter of passengers eligible for participation in the US VISIT were processed utilizing biometrics.

In addition to monitoring the exit program goals, the CBP has also indicated that it is looking to expand the audit programs for privacy compliance and technical accuracy in the operation of the matching system in response to a 2020 GAO audit of the developing CBP program.[30] This means that airports and airlines that are supporting the CBP exit program can anticipate additional guidance and audit requirements. For example, the GAO report noted some deficiencies with respect to the posting of signage informing passengers of the biometric screening processes and advising US citizens of their ability to opt out of such screening. An example of that signage is depicted in Figure 4.

Figure 4. CBP Exit Signage (Rev.2019)



U.S. Customs and
Border Protection

Privacy Information – Biometric Boarding

As you approach the e-gate or camera, your photograph will be taken and provided to U.S. Customs and Border Protection (CBP). CBP will compare that photograph to the image(s) associated with your passport, visa, other travel documents, or prior border inspections.

CBP will delete photographs of U.S. citizens collected through this process within 12 hours. For certain non-U.S. citizens, the photograph may be retained in secure Department of Homeland Security (DHS) systems and used as a biometric confirmation of departure from the United States as required by law (8 U.S.C. § 1365b; 8 C.F.R. 215.8(a)(1)).

All CBP partners – such as airports, air carriers, their system integrators and/or vendors – will immediately delete any photos taken during this process. These entities will not retain any photograph taken during boarding for any purpose and are subject to DHS compliance audits.

If you do not wish to have your picture taken, please see a gate agent or CBP officer to request alternative procedures for identity verification and/or biometric confirmation of departure from the United States.

For more information, please visit our website at www.cbp.gov/biometrics.

CBP Publication No. 0861-0619
Revised Month 2019

Source: CBP.gov

CBP noted that while it exercises control over the FIS areas to post signage relative to screening on entry, the departure areas of airports where signage relative to exit is required to be posted is outside their operational control. In response to the 2020 GAO report, CBP stated its intent to work with airports and airlines to ensure the posting of required privacy notifications.

The CBP initiative to automate biometric screening at departure gates offers both benefits and burdens for airports and airlines. On the positive side, the use of biometrics through the TVS provides a quick,

[30] U.S. General Accountability Office 2020. "Facial Recognition CBP and TSA are Taking Steps to Implement Programs, but CBP should Address Privacy and System Performance Issues." *GAO-20-568.* Washington D.C. Cited at https://www.gao.gov/assets/gao-20-568.pdf.

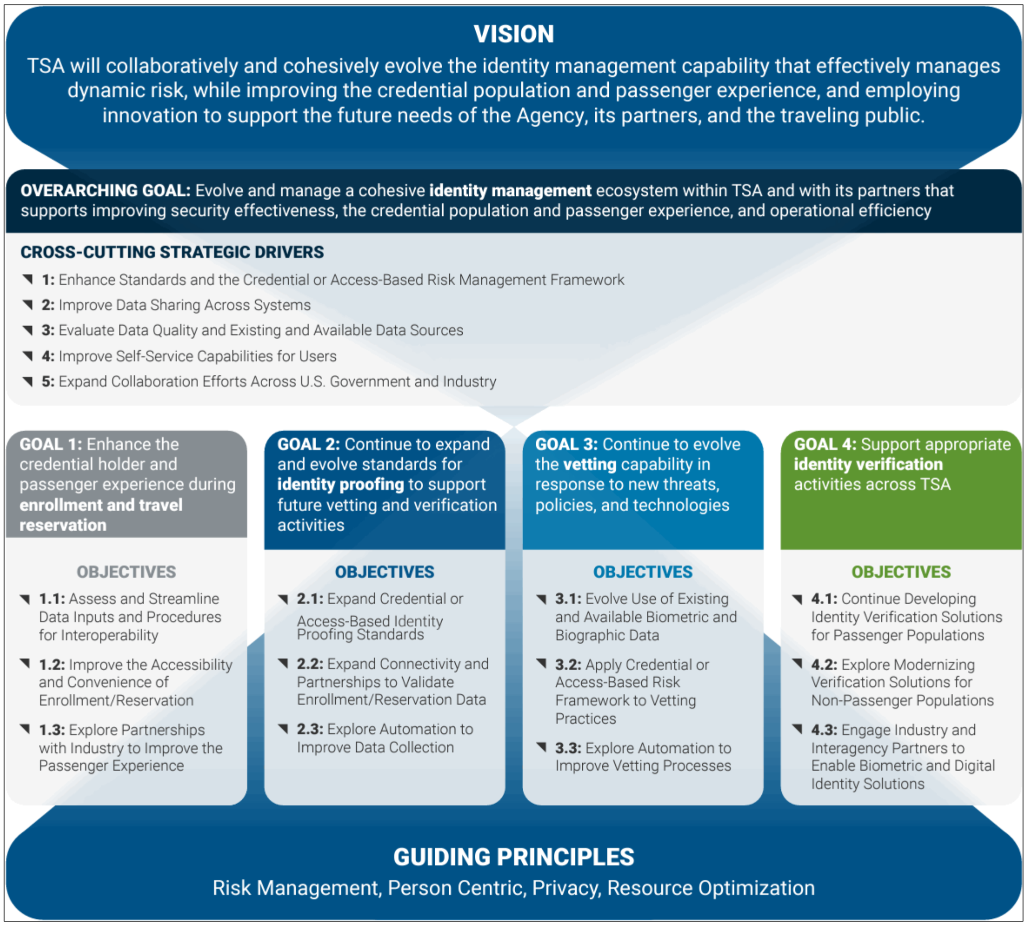
touchless boarding process. On the other hand, automation of the process will require airports and airlines to align their operations with TVS business, technical, and privacy requirements, and to procure, install, and operate necessary equipment and software.

3.3.2 TSA Credential Authentication Technology and PreCheck® Enhancement

TSA has developed plans to enhance security operations through automated biometric screening measures. Through their *Biometric Roadmap* (2018)[31] and *Identity Management Roadmap* (2022),[32] as well as presentations to various industry groups, TSA has outlined its approach to automating the passenger identity verification process and its commitment to strengthening identity management in other aspects of security, such as aviation worker screening.

TSA's *Biometric Roadmap* focuses on the implementation of biometrics in connection with passenger journey. *Identity Management Roadmap* builds on this by presenting visions and goals for creating a system within TSA and its partners to improve the strength and efficiency of aviation worker credentialing and the passenger experience. It deals with concerns over issues of registration and enrollment, proofing, vetting, and verification. The vision and goals are outlined in Figure 5.

Figure 5. TSA Identity Management Vision and Goals



VISION

TSA will collaboratively and cohesively evolve the identity management capability that effectively manages dynamic risk, while improving the credential population and passenger experience, and employing innovation to support the future needs of the Agency, its partners, and the traveling public.

OVERARCHING GOAL: Evolve and manage a cohesive **identity management** ecosystem within TSA and with its partners that supports improving security effectiveness, the credential population and passenger experience, and operational efficiency

CROSS-CUTTING STRATEGIC DRIVERS

- **1:** Enhance Standards and the Credential or Access-Based Risk Management Framework
- **2:** Improve Data Sharing Across Systems
- **3:** Evaluate Data Quality and Existing and Available Data Sources
- **4:** Improve Self-Service Capabilities for Users
- **5:** Expand Collaboration Efforts Across U.S. Government and Industry

GOAL 1: Enhance the credential holder and passenger experience during **enrollment and travel reservation**

OBJECTIVES

- **1.1:** Assess and Streamline Data Inputs and Procedures for Interoperability
- **1.2:** Improve the Accessibility and Convenience of Enrollment/Reservation
- **1.3:** Explore Partnerships with Industry to Improve the Passenger Experience

GOAL 2: Continue to expand and evolve standards for **identity proofing** to support future vetting and verification activities

OBJECTIVES

- **2.1:** Expand Credential or Access-Based Identity Proofing Standards
- **2.2:** Expand Connectivity and Partnerships to Validate Enrollment/Reservation Data
- **2.3:** Explore Automation to Improve Data Collection

GOAL 3: Continue to evolve the **vetting** capability in response to new threats, policies, and technologies

OBJECTIVES

- **3.1:** Evolve Use of Existing and Available Biometric and Biographic Data
- **3.2:** Apply Credential or Access-Based Risk Framework to Vetting Practices
- **3.3:** Explore Automation to Improve Vetting Processes

GOAL 4: Support appropriate **identity verification** activities across TSA

OBJECTIVES

- **4.1:** Continue Developing Identity Verification Solutions for Passenger Populations
- **4.2:** Explore Modernizing Verification Solutions for Non-Passenger Populations
- **4.3:** Engage Industry and Interagency Partners to Enable Biometric and Digital Identity Solutions

GUIDING PRINCIPLES

Risk Management, Person Centric, Privacy, Resource Optimization

Source: TSA Identity Management Roadmap (2022)

[31] Transportation Security Administration 2018. "TSA Biometric Roadmap, For Aviation Security & the Passenger Experience," p.18. Cited https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[32] Transportation Security Administration 2022. "TSA Identity Management Roadmap," Washington D.C. at p. 24. Cited at https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf.

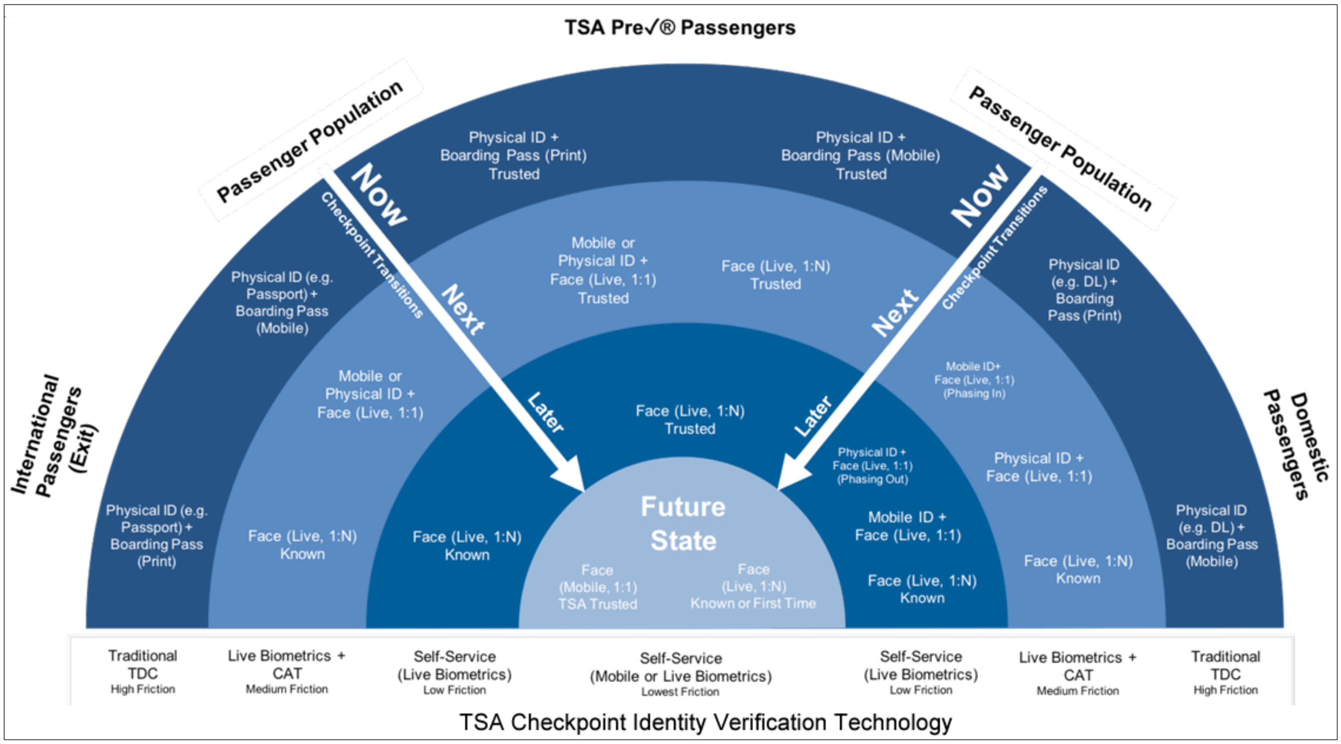
TSA has not provided specific guidance for biometric use in the verification of non-passenger populations. The regulatory authority to mandate such processes remains unclear.

With respect to passenger populations, consonant with the visions and goals outlined in Figure 5 above, TSA is pursuing the introduction of biometrics in connection with passenger processing. The process outlined in the *Biometric Roadmap* includes the achievement of four principal goals:

1. Partnering with CBP on biometrics for international travelers
2. Operationalizing biometrics for TSA PreCheck travelers
3. Expanding biometrics to domestic travelers
4. Developing support infrastructure for biometric solutions

In pursuit of those goals, TSA is following the phased approach depicted in Figure 6.

Figure 6. TSA's Phased Approach to Biometric Implementation in the Passenger Journey[33]


TSA Pre✓® Passengers
Passenger Population
Passenger Population
International Passengers (Exit)
Domestic Passengers
Now
Next
Later
Checkpoint Transitions
Now
Next
Later
Checkpoint Transitions
Physical ID + Boarding Pass (Print) Trusted
Physical ID + Boarding Pass (Mobile) Trusted
Physical ID (e.g. Passport) + Boarding Pass (Mobile)
Mobile or Physical ID + Face (Live, 1:1) Trusted
Face (Live, 1:N) Trusted
Physical ID (e.g. DL) + Boarding Pass (Print)
Mobile or Physical ID + Face (Live, 1:1)
Mobile ID+ Face (Live, 1:1) (Phasing In)
Face (Live, 1:N) Trusted
Physical ID + Face (Live, 1:1) (Phasing Out)
Physical ID + Face (Live, 1:1)
Physical ID (e.g. Passport) + Boarding Pass (Print)
Face (Live, 1:N) Known
Face (Live, 1:N) Known
Future State
Face (Mobile, 1:1) TSA Trusted
Face (Live, 1:N) Known or First Time
Mobile ID + Face (Live, 1:1)
Face (Live, 1:N) Known
Face (Live, 1:N) Known
Physical ID (e.g. DL) + Boarding Pass (Mobile)
Traditional TDC High Friction
Live Biometrics + CAT Medium Friction
Self-Service (Live Biometrics) Low Friction
Self-Service (Mobile or Live Biometrics) Lowest Friction
Self-Service (Live Biometrics) Low Friction
Live Biometrics + CAT Medium Friction
Traditional TDC High Friction
TSA Checkpoint Identity Verification Technology

Source: TSA *Biometric Roadmap* (2018)

The phased approach moves away from verification processes that involve extensive TSA personnel involvement and toward automated processes that are largely self-service. The movement along the continuum is characterized by reduced operational friction as automation increases.

For example, TSA is working to automate the role of Transportation Security Officers (TSO) who check documents at the checkpoint. These officers verify the identities of travelers by visual inspection of the identity documents they produce (e.g., drivers' licenses, passports) to determine their authenticity and to compare the photo and information on the identification document with the traveler and their boarding

[33] Transportation Security Administration 2018. "TSA Biometric Roadmap, For Aviation Security & the Passenger Experience." Cited https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

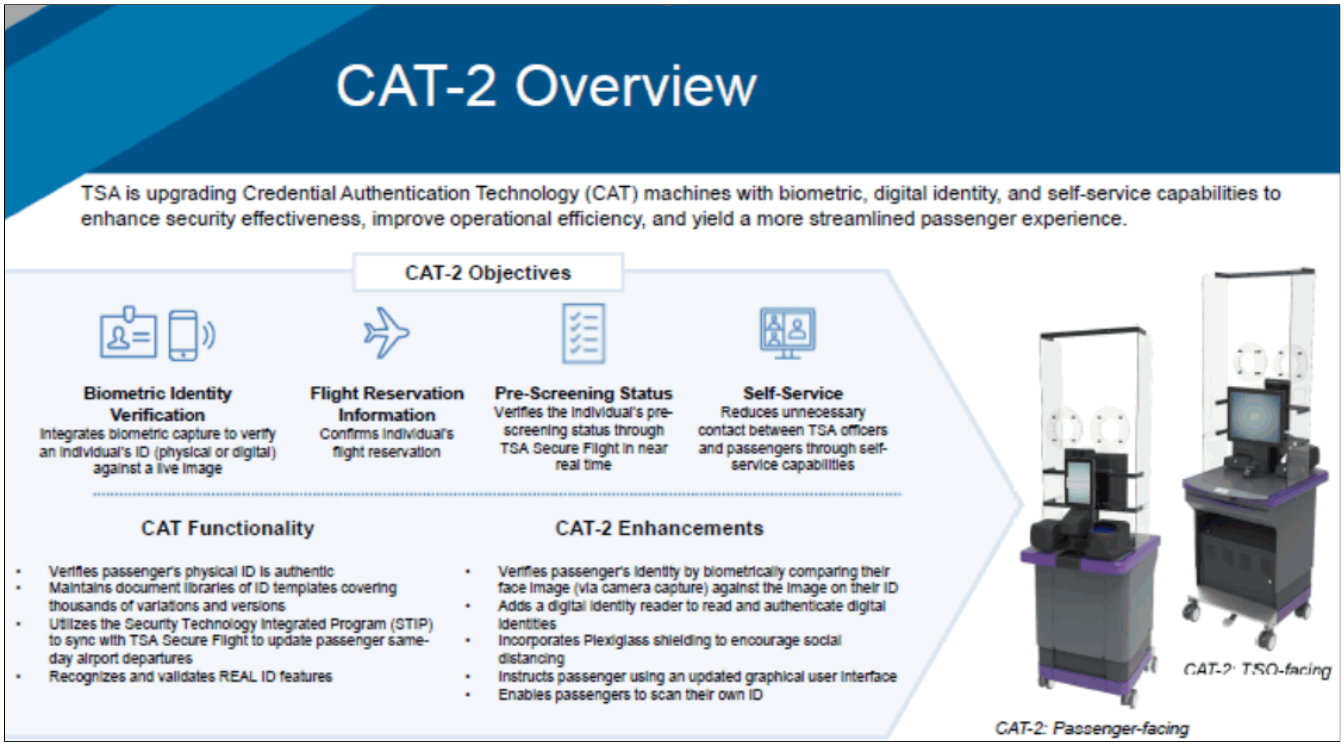
pass. Replacing the agent with a biometric application in the document check process has the potential to speed transactions, reduce labor requirements, and increase verification accuracy.

However, it has raised concerns by privacy advocates regarding government collection of biometric images. To address these concerns, TSA has made participation in biometric programs optional for travelers, and has placed limits on the length of time images used in biometric verification can be retained. This will necessitate different processes for verification of passengers who opt out of biometric processing, including different processing equipment, queueing, staffing, and space requirements.

Central to the biometric process is TSA's CAT, which introduced the automated capability to establish authenticity of identity documents and conduct a verification against No-Fly information. The initial CAT deployments still required the TSO at each checkpoint lane to physically inspect the identity document to compare the photograph of the document to the face of the traveler being processed.

CAT has evolved as part of TSA's phased roadmap. Building on the initial CAT capability, TSA is upgrading the automated identity verification process through the introduction of CAT-2. A comparison of the capabilities of the original CAT system with the new CAT-2 system is provided in Figure 7.

Figure 7. CAT and CAT-2 Comparison



CAT-2 Overview

TSA is upgrading Credential Authentication Technology (CAT) machines with biometric, digital identity, and self-service capabilities to enhance security effectiveness, improve operational efficiency, and yield a more streamlined passenger experience.

CAT-2 Objectives

Biometric Identity Verification
Integrates biometric capture to verify an individual's ID (physical or digital) against a live image

Flight Reservation Information
Confirms individual's flight reservation

Pre-Screening Status
Verifies the individual's pre-screening status through TSA Secure Flight in near real time

Self-Service
Reduces unnecessary contact between TSA officers and passengers through self-service capabilities

CAT Functionality

- Verifies passenger's physical ID is authentic
- Maintains document libraries of ID templates covering thousands of variations and versions
- Utilizes the Security Technology Integrated Program (STIP) to sync with TSA Secure Flight to update passenger same-day airport departures
- Recognizes and validates REAL ID features

CAT-2 Enhancements

- Verifies passenger's identity by biometrically comparing their face image (via camera capture) against the image on their ID
- Adds a digital identity reader to read and authenticate digital identities
- Incorporates Plexiglass shielding to encourage social distancing
- Instructs passenger using an updated graphical user interface
- Enables passengers to scan their own ID

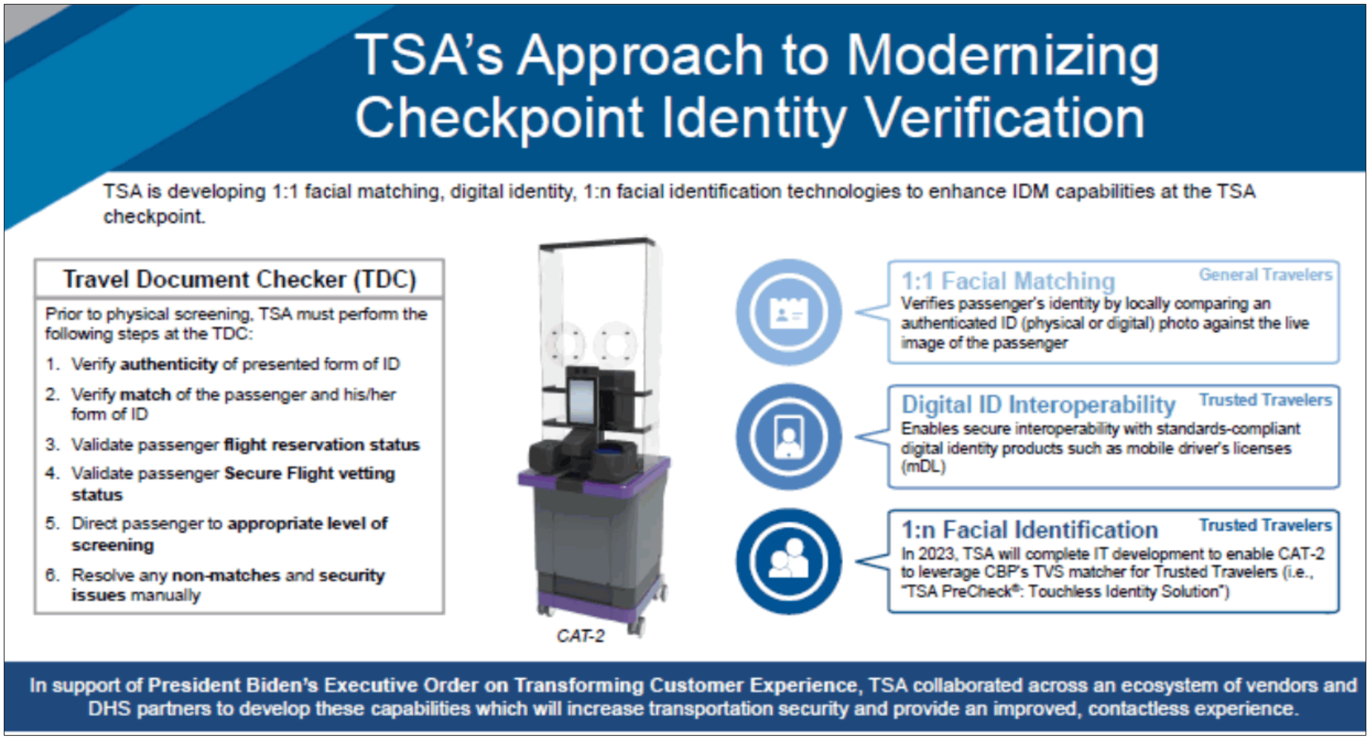
Source: TSA Identity Management Presentation

The CAT-2 technology will be able to establish the authenticity of travel documents as well as query electronic records to identify the individual as a ticketed passenger. This eliminates the need to check boarding passes. Additionally, CAT-2 has facial recognition technology that can match images of the traveler being processed to the photograph on the identity document or images stored in digital identity applications on mobile devices.

The final phase of the TSA CAT system will be to move away from comparing passenger images with physical or digital identity documents to a process that compares those images to galleries of photographs stored in CBP's TVS database. This process would be like passenger processing using e-gates for departure at boarding gates.

There is currently no mechanism to enroll passengers into the TVS database except through CBP processes in connection with international travel. While that database currently can access all passport images, individuals without passports would have to enroll their images. TSA is looking to create this enrollment process. As a first step, TSA is developing an enrollment path through its TSA PreCheck program. As of June 2023, this is still a pilot initiative at a couple of select airports, but it could later be expanded to other airports. Images taken of TSA PreCheck passengers who volunteer to enroll are uploaded to the TVS database. The goal of this program is to allow for the processing of passengers utilizing only their facial image; no physical or digital identity documentation would be required. The figure below depicts the evolution of CAT -2 processing from 1:1 comparisons to a 1:N process.

Figure 8. TSA's Checkpoint Identity Verification



TSA's Approach to Modernizing Checkpoint Identity Verification

TSA is developing 1:1 facial matching, digital identity, 1:n facial identification technologies to enhance IDM capabilities at the TSA checkpoint.

Travel Document Checker (TDC)

Prior to physical screening, TSA must perform the following steps at the TDC:

1. Verify **authenticity** of presented form of ID
2. Verify **match** of the passenger and his/her form of ID
3. Validate passenger **flight reservation status**
4. Validate passenger **Secure Flight vetting status**
5. Direct passenger to **appropriate level of screening**
6. Resolve any **non-matches** and **security issues** manually

1:1 Facial Matching General Travelers

Verifies passenger's identity by locally comparing an authenticated ID (physical or digital) photo against the live image of the passenger

Digital ID Interoperability Trusted Travelers

Enables secure interoperability with standards-compliant digital identity products such as mobile driver's licenses (mDL)

1:n Facial Identification Trusted Travelers

In 2023, TSA will complete IT development to enable CAT-2 to leverage CBP's TVS matcher for Trusted Travelers (i.e., "TSA PreCheck®: Touchless Identity Solution")

In support of President Biden's Executive Order on Transforming Customer Experience, TSA collaborated across an ecosystem of vendors and DHS partners to develop these capabilities which will increase transportation security and provide an improved, contactless experience.

Source: TSA Identity Management Presentation

The incorporation of new facial recognition technology into TSA screening checkpoint operations will likely require reconfiguration of TSA checkpoint operation space and the adjoining queueing space. However, until TSA's pilot programs are completed, the exact parameters of those changes will be difficult to gauge. The pilots should demonstrate not only the footprint needed to accommodate the new technology, but also the public adoption level of that technology.

Understanding public adoption levels will be particularly important to assessing the allocation of queueing space and hardware systems. Given the ability of passengers to opt-out of biometric processes, understanding the preference of passengers for those processes and configuring space and equipment accordingly will be critical challenges. While the decisions in those matters will be executed by TSA, the accommodations in terms of facility operations will be placed on the airports.

3.3.3 GAO Recommendations on Biometric Enhancements

Two 2020 GAO reports provide insight into potential future requirements for biometric enhancements for both access control and passenger journey. In a February 2020 report addressing TSA efforts to address insider threat concerns, the GAO notes the incorporation of biometrics into access control measures.[34] The TSA *Insider Threat Roadmap* published later in 2020, which cited the February GAO report, observed that technology improvements might assist in strengthening insider threat mitigation measures. Subsequently, in the 2022 *Identity Management Roadmap*, the TSA notes the importance of biometrics in non-passenger security contexts. While none of these TSA pronouncements mandate biometric use in conjunction with required access control measures, they indicate an organizational shift in favor of such practices and the potential for future guidance with respect to those practices.

In a September 2020 GAO report analyzing CBP and TSA programs for passenger processing, the GAO noted the strength of TSA efforts to provide privacy protections in connection with its pilot programs.[35] The report noted that TSA had completed and posted on its website detailed PIAs for each of its pilots following Fair Information Practice Principles (FIPP). The pilot programs provide notice to the public of the objectives of the pilots and the ability of passengers to opt-out. The PIAs also include information on the PII data collected, the length of retention, and disposal of the data.

The findings of this GAO report with respect to TSA and CBP point to the importance of ensuring privacy with respect to biometrics in the passenger processing context. This includes the conduct of PIAs utilizing FIPPs prior to implementation of programs, as well as audit and review of programs subsequent to their implementation. It also includes ensuring that passengers have adequate notice of the programs and information regarding their right to opt out of the programs.

3.4 Digital Identification Applications

Digital ID has been endorsed by TSA and some airlines for authenticating passenger identity, and are referenced on the TSA website as part of their technology initiatives to promote "…a faster, easier travel experience."[36] Digital IDs are established through applications on mobile devices offered by governmental or trusted third-party entities. The applications establish identity of the device holder. They can provide a fast and accurate way to authenticate identity against verifiable identification documents. They also provide a privacy shield from disclosure of information that is not relevant to the authentication process.

The application links the face of the digital ID holder to an acceptable travel document that has been inspected and authenticated through the application. In the travel process, the application can substitute for a travel document to establish identity, such as a driver's license or a passport. Rather than presenting physical copies of those travel documents, identity is authenticated through the application. The TSA accepts digital IDs in lieu of travel documents at certain airports where the checkpoints are equipped with CAT-2 technology.

Digital ID enrollment requires the user to provide a photograph of an identity document such as a passport or driver's license. The individual seeking to establish the digital ID then uploads a photo of

[34] General Accountability Office 2022. "TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals" Washington D.C., p. 25, figure 3. Cited at https://www.gao.gov/assets/gao-20-275.pdf.
[35] U.S. General Accountability Office 2020. "Facial Recognition CBP and TSA are Taking Steps to Implement Programs, but CBP should Address Privacy and System Performance Issues." *GAO-20-568.* Washington D.C. Cited at https://www.gao.gov/assets/gao-20-568.pdf.
[36] Transportation Security Administration. "Biometric and Digital Identity Solutions for TSA PreCheck Members." *TSA Official Website*. Cited at Digital ID | Transportation Security Administration (tsa.gov).

themselves to the application. The application authenticates the identity document and then, using facial recognition technology, compares the photograph on the verified document to the uploaded photograph. Once a match is established, the digital ID is created within the application. It can only be utilized on the device on which it is created, and it is not transferrable from one device to another. If the device is not available (e.g., lost, stolen, or damaged), the digital ID needs to be established on a new device.

A digital ID allows the user to determine with whom they will share their identity information. In many cases, the digital ID owner can also specify the information to be shared. For example, a physical driver's license may have information such as height, eye color, and weight, which will be made available to the entity checking the document. A digital ID allows the information owner to shield that information. The QR code will only reveal that there is a valid digital identity matching the person who is presenting the digital ID.

In instances where TSA is accepting digital IDs, the traveler presents the QR code in their digital ID application. Facial recognition technology in the CAT-2 machine matches data from the image of the person presenting the digital ID with the image stored on the application. If the image matches, the individual is permitted to process thought the checkpoint.

Arizona[37], Utah,[38] and Maryland[39] have also worked to develop mobile driver's licenses. These programs establish digital IDs utilizing the driver's license of their respective state. The state departments regulating motor vehicle licensure operate websites that describe the enrollment practices and uses of these mobile driver's licenses. The mobile driver's licenses from these states can also be used in the airports accepting digital IDs at TSA checkpoints.[40]

Airlines are also looking at utilizing digital IDs with other portions of the passenger journey. For example, one air carrier has created a digital ID for use at bag drop, utilizing readers and facial recognition technology similar to the TSA checkpoint. One airport is piloting the use of digital ID in connection with a complete curb-to-gate solution for passenger processing.

Digital ID programs are voluntary and require that users have a smartphone device or tablet capable of operating the application. The national and international standards that address data security issues around digital IDs should be considered with respect the use of any particular digital ID.[41]

[37] Arizona Department of Transportation, "Mobile ID", *Official Website*, Cited at https://azdot.gov/mvd/services/driver-services/mobile-id.

[38] Utah Department of Public Safety, "Utah Mobile Driver's License (mDL) Program", *Official Website*, Cited at https://dld.utah.gov/utahmdl.

[39] Maryland Department of Transportation, "Maryland Mobile ID in Apple Wallet", *Official Website*, Cited at https://mva.maryland.gov/Pages/MDMobileID_Apple.aspx.

[40] See, TSA "Biometric and Digital Identity Solutions for TSA PreCheck Members" *supra*, n. ___.

[41] See, e.g. National Institute of Standards and Technology, "Digital Identity Guidelines" *NIST Special Publication 800-63-3* (June 2017), cited at Digital Identity Guidelines (nist.gov); and International Standards Organization, "Personal Identification—ISO—Complaint Driving Licence—Part 5 Mobile Driving License (mDL) Application" *ISO/IEC 18013-5:2021* (2021) Cited at https://www.iso.org/standard/69084.html.

SECTION 4: IMPLEMENTING BIOMETRICS FOR ACCESS CONTROL

When considering the implementation of biometrics for access control at an airport, numerous considerations should be taken into account, as listed in the following sections. It is important to engage with relevant stakeholders, including airport management, security personnel, IT departments, legal experts, and privacy advocates, to address all the process considerations effectively and ensure a successful implementation of biometrics for access control at the airport.

4.1 Needs Assessment and Requirements Development

Common sentiments regarding needs assessments and requirements development were related to baseline studies, goals and objectives, and stakeholder participation.

- Perform a baseline study of existing processes to measure improvement. Consider introducing behavioral science in addition to industrial engineering to assess biometric processes.
- Increased efficiency is an important goal but may not be the most important objective. There are other considerations as to why an airport may look at biometrics, including security enhancement, user acceptance, regulatory/compliance, and reputation.
- Environmental factors such as temperature, humidity, air pressure, lighting, and obstructions can all impact the accuracy of biometric systems. Ensuring that these conditions are carefully considered when preparing for installation is crucial for achieving optimal performance.
- Recognize that biometric devices are not needed on every portal. Be sure to consider one or more of the following:
    - Security needs of the access point. For example, unauthorized access to a communications closet could cause a major issue with more than one airport operation versus unauthorized access to a small janitorial closet, which could only cause a minor disruption to a single process. Implementing biometrics in higher risk areas can enhance security and provide additional security assurances.
    - Operating environment where the biometrics are to be deployed (e.g., cold versus warm weather clothing, working areas requiring gloves, etc.). This may drive where biometrics are deployed as well as what biometric is chosen.
    - User population experience and preferences. Generally, this would favor use of a fingerprint biometric due to the familiarity of aviation workers with that biometric. However, changing use patterns in other sectors, such as the use of facial biometrics in smart devices, may alter the calculus of familiarity with biometric processes.
- Conduct in-depth research on biometric solutions before implementation.
- Consider the existing access control infrastructure and understand that some legacy systems may require upgrades prior to deploying biometric technology; those upgrades will need to be incorporated into the program plan.
    - Based in part on existing physical infrastructure (power, cabling, etc.), biometric solutions may not be feasible or economically justifiable for every portal.
    - Infrastructure limitations may also restrict the ability of airports to utilize certain types of biometric access control technology.

- The use of biometrics can help meet ID media audit requirements more efficiently and also provide tools for improved badging accountability. These practices are discussed in PARAS 0020 – *Strategies for Effective Airport Identification Media Accountability and Control*.[42]
- Before selecting a system vendor, airports should first select the appropriate biometric modality based on the intended application. For example, when used for access control, consideration should be given to the environment where the reader will be located. Some biometric modalities may not perform well in extreme heat and cold or direct sunlight.

4.2 Selection Criteria

Biometric technology is best viewed as a component in an integrated system. Some vendors offer complete systems that include a biometric component. Such a solution reduces the burden and risk of a custom integration process.

Independent product test data should be reviewed before vendor selection. For example, NIST conducts comparative performance testing of face, fingerprint, and iris biometric modalities using large-scale common data sets, and publishes the results for public access. Further, the DHS Science and Technology Directorate has partnered with CBP to host Biometric Technology Rallies to test and evaluate biometric technologies at its Maryland Test Facility. The test scenarios include human subject testing that simulates operational conditions such as those that would be encountered at an airport.[43]

When possible, contact current users of biometric systems that are deployed in similar applications as is contemplated by the airport. It is best to communicate directly with the system owner and/or visit the site to understand the considerations that were used in the biometric selection process. This would be an excellent opportunity to observe system performance and to find out any lessons learned that can be applied to the airport's selection criteria.

When selecting a device manufacturer, in addition to system features, functionality, and compatibility with existing systems, airports should consider the roadmap of both the device and its manufacturer, annual maintenance costs, recurring licensing fees, system updates, and other recurring costs associated with the proposed system. Airports also need to understand how long they can expect a reliable supply of replacement parts, service, and support over the anticipated life cycle of the selected system. RFPs should require that proposals include the following information:

Company Stability and Longevity – A company's financial stability and longevity in the industry speaks to the probability that they will continue to support and manufacture products. Equally important is the manufacturer's experience in biometric access control in an airport environment, and their expertise in airport regulations and best practices.

Company Track Record of Innovation and Delivery – As the technology market advances and vendors improve their products, they may cease to produce and/or support the technologies that have been deployed. This can lead to challenges in securing replacement products or supporting operations. To mitigate this, airports should consider manufacturer/vendor roadmaps for product development. Look at their history, including how previous device models were decommissioned and supported both in terms of parts and service. Several case studies had issues with device manufacturers discontinuing a device or significantly changing components, leaving the airports hamstrung in their ability to procure

[42] **PARAS 0020:** https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf.
[43] **Biometric Technology Rally:** https://www.dhs.gov/science-and-technology/biometric-technology-rally.

new parts and/or service for the deployed devices. In one case, this caused the airport to have to redesign their program well before the anticipated end-of-life of the initial deployment.

Security Posture – Look for a Secure Software Development Life Cycle and a Privacy by Design (PbD) approach where privacy considerations are taken into account at the outset and not as an afterthought in development. See Section 6.5 for more details about PbD.

Installation and Integration – Physical infrastructure and compatibility with existing security systems can limit technology choices. Ensure the device allows for open integration and has a published Software Development Kit or Application Programming Interface (API), ensuring there is no requirement to use a proprietary application or device hardware.

Scalability – Ensure the system accommodates planned future growth and changes in user volumes. The system should be able to handle increasing enrollments, authentication requests, and system upgrades.

Life-Cycle Costs – In addition to initial setup costs, including hardware, software, training, and integration expenses, airports should consider ongoing maintenance, licensing fees, system upgrades, and eventual obsolescence when assessing the overall cost of implementation.

In this era of rapid technological advances, the normal life cycle of technology requires an almost continuous review of biometric access control products. The length of time needed to procure and deploy biometric systems within complex access control and security systems means the length of time those readers can remain in active service is relatively short.

User Acceptance – External considerations such as local political and community concerns over the application of certain biometric technologies, such as facial biometrics, can constrain selection choices.

4.3 Procurement

The cost and size of most biometric access control projects may mean that product selection will be conducted through a competitive procurement process.

While procurement processes will vary from airport to airport, they often involve interdisciplinary committees of stakeholders from across the airport community, including security, finance, and operations personnel. The composition of procurement selection committees means that factors beyond security efficiency are considered, including fiscal impact, existing contract relationships, and diversity.

Often the selection of biometric reader technology is in connection with a larger procurement of a complete access control system. This approach can result in:

- Tradeoffs among systems (e.g., accepting a biometric solution with more limited functions because it is offered in conjunction with an access control system that has other desirable features)
- The benefit of a holistic system offering that presents a single entity responsible for ensuring system integration
- Attenuation of direct security considerations in system selection

4.4 Product Review and Testing

Once one or more candidate systems are identified, the airport may consider collaborating with the system vendors to conduct limited testing at the airport to measure performance under simulated or actual operational conditions. This would be particularly helpful if the use case is novel and/or there are few reference users that can be conveniently contacted or visited. An evaluation of biometric systems should take into account a number of factors, including:

Standardization of test criteria: Standardizing evaluation criteria and methodologies across all systems can facilitate comparisons and ensure the systems are tested objectively.

Multimodal capabilities: When testing systems that support multiple biometric modalities (e.g., fingerprint, face, iris) each modality's performance should be evaluated individually and in combination.

Real-world conditions: Testing should account for conditions that reflect and actual deployment, such as lighting, environmental factors, and user demographics and behavior.

The location of biometric technology must be also considered. For example systems installed outdoors in cold climates may affect individuals' ability to interact with technologies such as fingerprint readers, which would require users to remove their gloves to access the technology. The general operating environment, including from dirt and obstructions, network connectivity, and potential electromagnetic interference should also be reviewed.

Care should also be taken to ensure that the system will accommodate all users including those that may have difficulty presenting a biometric sample that the sensor can acquire.

Altered/Excepted Conditions: Testing should also examine any deviations from the normal, expected conditions that may result in failure to enroll, failure to acquire, or false rejections. For example, Extreme temperatures and high humidity can impact both the device and the clarity of the captured biometric. Low or harsh lighting conditions can also hinder the capture of facial or eye images. Alterations to the user's biometric, such as dirt or injury on a presented finger, or glasses on a face, may also affect acceptance rates of authorized users.

Performance Metrics: Define appropriate performance metrics, including accuracy, false acceptance/rejection rates, response times, and usability.

User Experience Assessment: Expanding testing to include the evaluation of user experience aspects such as ease of use, user satisfaction, and usability can provide valuable insights. Balancing security and efficiency while providing a positive user experience is essential. User-friendly interfaces, clear instructions, and minimizing authentication time are crucial to ensure smooth and convenient experiences for users.

Security and Vulnerability Assessment: Conducting comprehensive security testing to identify potential vulnerabilities, such as spoofing or tampering risks, can help ensure that biometric access control systems are robust and resistant to attacks.

Collaboration with Users: Involving end users such as airport personnel and security staff in the testing process by collecting feedback, and conducting user surveys and user trials can provide valuable insights into the practical performance and usability of the systems.

Airports may develop their own testing program or engage a consultant to manage the evaluation. Safe Skies' ASSIST program is also available to airports to test and evaluate biometric devices on site. The program operates at no cost to airports and provides detailed results for each system evaluated in the airport's operating environment.

Ongoing and periodic evaluation of biometric access control systems can drive improvements and identify vulnerabilities, allowing for timely updates, patches, and advancements in system performance and security. As with selection testing, this can be conducted by the airport or a consultant, or in collaboration with Safe Skies' POST (Performance and Operational System Testing) program, which provides ongoing testing and performance tracking of airport-owned security systems at no cost to airports.

4.5 Technology and Integrations

For many airports, the introduction of biometrics requires technological and process integrations with several differing systems, including:

- Hardware and software operating the access control system
- Hardware and software used in conjunction with ID media issuance
- Hardware and software used for identity management systems

The integration of these systems can be complex and, in some cases, a proprietary subsystem may not be capable of integrating with biometrics. Implementing biometric access control may also require significant infrastructure upgrades, including the installation of biometric enrollment devices, biometric readers, and backend systems. When a biometric technology is introduced in the context of a complete system upgrade there are reduced compatibility concerns, but a planned pilot period is the best opportunity to test the integration of new biometrics into an existing system or a newly designed one.

Due to the vast number of differing access control systems, ID media issuance systems, identity management systems, biometric systems, and the combinations of those systems in any given airport, it is impossible to provide precise integration guidance for biometrics beyond the requirement that all the subsystems must be analyzed for the ability to accept the introduction of any given biometric technology and process.

Many airports noted that they used a single systems integrator to plan and execute the deployment of a biometric technology as part of a larger security system. It was also common to use external contractors to perform systems integration functions in support of the deployment and maintenance of biometric technology.

It should also be noted that the introduction of biometric technologies into an existing system network may alter performance factors for the biometric technology and underlying systems, such as accuracy, reliability, and processing time. Airports should be mindful that performance specifications for biometrics need to be tested and confirmed in the context of the large ecosystem in which they will operate.

CUSTOM INTEGRATIONS

Integrating biometric access control with existing airport systems may require custom development, API integration, or data migration to ensure seamless data flow and interoperability between badging and the access control system. It is important to vet such integration requirements first to understand all program requirements and scopes of work (resources and cost). It is critical to ensure that the access control system the airport is using can support biometrics.

Any customizations should be reviewed carefully as they can impact the system administration, operation, and maintenance costs. Pitfalls to be wary of include:

- **Compatibility** related to legacy protocols, middleware, and adapters that may be used to bridge gaps between systems.
- **Security** risks related to the introduction of vulnerabilities in software and infrastructure.
- **Higher development and maintenance costs** especially if code is not standard or well documented. It is also possible to void manufacturer warranties and support depending on the customization performed. Customizations should follow best practices and adhere to common development workflows.
- **Vendor Dependency** is a potential outcome when customizing a system, which can create future support challenges.

DATA STORAGE AND PROTECTION

Develop robust protocols for secure storage and protection of biometric data. Implement encryption, access controls, and monitoring mechanisms to prevent unauthorized access or data breaches. Consider whether data will be stored locally or in a centralized system.

Additionally, running the access control system on a closed, secure network offers significant benefits:

Enhanced Security: Closed networks are isolated from external connections, making them less susceptible to unauthorized access or external attacks.

Reduced Vulnerability to Cyber Threats: Limiting external access reduces exposure to cyber threats such as malware, phishing attacks, and Denial of Service attacks, that could compromise the security of employee personal and biometric data or the entire system. Even insider threat is reduced due to the ease of tracking and monitoring activities on a closed system.

Reduced Attack Surface: The attack surface is the area of a system that can potentially be targeted in an attack. In a closed network, the attack surface is smaller because there are fewer entry points.

Easier Monitoring and Control: With fewer entry points and devices connected to the network, it is easier for administrators to monitor and control network activity. This allows for more efficient detection of anomalies or suspicious behavior.

Reduced Latency: Closed networks tend to have lower latency compared to open networks, as there is less traffic and congestion. This can lead to faster biometric authentication.

Better Scalability: Closed networks can be designed with scalability in mind, making it easier to expand the system as needed without compromising security.

Compliance with Regulations: A closed network can be designed to meet compliance requirements more effectively. Many industries have developed and are developing strict regulations regarding the handling and storage of sensitive data, including biometric information.

BADGE MEDIA

Implementing a new badge may be necessary for some biometric systems. Selecting the badge media to be used with biometric access control has its own subset of considerations. These considerations will also factor in with the decision on methodology of biometric verification, whether the biometric is stored on the badge media (i.e., smart card), in a database, or both.

- **Card Technology:** Evaluate the card technologies available, such as contact-based (e.g., chip) or contactless (e.g., RFID or near -field communication). Consider the advantages and disadvantages of each technology in terms of security, convenience, compatibility, and cost.

- **Biometric Integration:** If implementing a smart card, ensure the card is compatible with the selected biometric system, and that the card's capacity and processing capabilities are sufficient.
- **Security Features:** Examine the card's security features. Look for features like encryption, secure key management, tamper resistance, and secure storage of biometric templates (smart card only). Consider whether the card meets relevant security standards and certifications.
- **Card Life Cycle Management:** Consider the management of the cards throughout their life cycle. Evaluate the ease of card issuance, replacement, and revocation processes. If using a smart card, determine whether the card technology supports remote updates or if physical access to the card is required for updates and maintenance.
- **Compatibility and Integration:** Assess the compatibility and integration of the badge media with existing access control systems, infrastructure, and databases. Ensure that the cards can be seamlessly integrated into the overall access control ecosystem, including card readers, backend systems, and identity management platforms.
- **User Experience:** The card should be user friendly and provide a seamless experience for both cardholders and security personnel. Consider factors such as card issuance and activation processes and ease of use. For smart cards, also consider speed of authentication.
- **Scalability and Futureproofing:** Consider the scalability of the card solution to accommodate future growth, additional functionalities, or changes in security requirements. Evaluate whether the technology allows for easy expansion or upgrading without significant disruptions or additional costs.
- **Cost Considerations:** Evaluate the overall cost of implementing and maintaining the badge media. Consider factors such as card production and personalization costs, card reader infrastructure, ongoing maintenance, and potential licensing fees. Compare the costs with the expected benefits and return on investment.
- **Standards and Interoperability:** Consider adherence to industry standards and protocols to ensure interoperability with other systems and technologies. Compliance with relevant standards can facilitate integration with existing infrastructure and enable future interoperability with other systems.
- **Vendor Selection:** Research and evaluate different vendors and solution providers. Consider their reputation, track record, expertise, and customer support capabilities. Look for references and customer testimonials to gain insights into their reliability and customer satisfaction levels.

4.6 Deployment

Communications are critical in deploying biometric systems. Starting communications early helps airport stakeholders and the user population understand the deployment program and corresponding changes. Even limited deployments will touch numerous other systems, particularly credentialing, as well as affect a large number of employees.

Before implementing a large-scale program, several airports found value in conducting a pilot program. Pilot programs allowed for field testing of the biometric device installation and configuration requirements, its performance/compatibility with the existing access control system, and insight into user adoption. While pilots cannot continue indefinitely, they should be conducted in a way to give a meaningful field assessment of the new system. The longer the pilot testing the greater the opportunity to gather relevant data. Identifying potential issues during the pilot allow for corrective actions to be taken in advance of full-scale deployment.

Strategies for deployment vary by airport. Deployment can be conducted in a phased approach, particularly in a replacement context. Some airports have used biometrics initially to secure the most critical facilities and then expanded to less critical locations. One airport interviewed for this study focused on deployment at all first-access points into Secured Areas or SIDA. Another airport focused on deployment in Sterile Areas and then expanded coverage to Secured Areas and SIDA. There were two common features of these deployments. First, they were based on security assessments of airport vulnerabilities and were targeted to remediate those vulnerabilities. Second, the deployments generally expanded out from initial deployment areas to additional areas of the airport.

System reliability and maintenance is also a concern. Regular maintenance, software updates, and hardware calibration are necessary to ensure system performance and accuracy. Planning for maintenance and support should be considered as part of the overall project.

Develop contingency plans for situations like system failures, power outages, or maintenance activities. Consider backup procedures, alternative access control methods, and communication protocols to minimize disruptions and ensure continuous operation.

ENROLLMENT

Prior to any biometric implementations, airports should understand the enrollment requirements and plan to enroll the entire airport population, or a subset depending on the biometric reader placement and employees authorized to use the access points.

Enrollment involves collecting and storing biometric data. It is crucial to communicate clearly with employees about what data is captured, how it is stored, and how data may be used. The airport should also establish a secure and efficient enrollment process, including obtaining necessary consent and protecting privacy. Airports can employ different enrollment strategies, including:

- All badge applicants can be enrolled
- Only applicants who will access portals with biometric readers can be enrolled
- Applicants for certain categories of badges can be enrolled (even if those individuals are not immediately granted access to those portals)

Enrolling individuals who will use portals secured with biometric readers does not necessarily mean that they will be granted access through all those portals. Access privileges can be restricted to only specified access points.

During biometric enrollment, an applicant’s biometric sample is captured and processed into a template for storage on a reader device, a smart card, and/or in the access control system server or field controller. This is necessary since all biometric matching takes place at the template level. Storing biometric templates also enhances privacy by limiting exposure of PII since templates do not reveal the original biometric data representation (e.g., bitmap image of a fingerprint pattern).

Consideration should also be given to the logistics of biometric enrollment. User enrollment usually involves an in-person visit to a facility where a trained operator assists the user in collecting a high-quality template. The incorporation of biometric enrollment with the badge issuance process is the common method for airports. A high-quality enrollment will result in reduced false rejections and increased overall system matching performance. Every effort should be made to ensure the highest possible biometric enrollment quality.

Procedures should also be implemented to test each biometric enrollment before the user leaves the enrollment station to ensure that the user can be matched successfully and that they are familiar with the procedure. The verification of the biometric in the badging office allows for an immediate assessment of the template's proper functioning and allows for orientation to the biometric readers.

It is also important to consider options for employees who cannot use a specific biometric modality or whose biometric data does not meet the accepted threshold. This will vary from airport to airport considering their policies, but also from manufacturer to manufacturer.

Some airports reported that fast tracking the enrollment process was a good decision for their implementations, especially those with large badge populations. In one case, the airport opened a separate office to handle only biometric enrollments for the existing population. The main credentialing office was then free to handle other badging needs such as new user processing, training, background checks, compliance, and user assistance.

One program used temporary personnel along with experienced managers and consultants to perform a fast-track enrollment process. Initially, errors were high but reduced substantially with retraining that keyed in on a checklist-type process to avoid reprints and field issues. Reports were run each day for managers to review data and adjust as needed.

TRAINING

Educating the user population of enrollment requirements as well as providing a high level explanation of the technology can improve the enrollment process and user adoption, and reduce issues when first using the biometric devices. Consider installing biometric devices in credentialing areas so users can test using the new devices immediately after enrollment. Be prepared to provide assistance and training at credential issuance. In some cases, it may be helpful to have written guidance posted near deployed devices for those devices that do not have onboard guidance. Feet appliqués in addition to instructional placards work best to assist users with facial recognition device operation.

When training credentialing personnel on enrollment procedures, teach them to follow the process the same way every time to reduce errors. Provide comprehensive training to airport staff who issue credentials. They should be proficient in system operation, troubleshooting, and understanding privacy considerations to address passenger queries or concerns effectively.

Include all safety and security personnel in training so they understand how to use the devices, where the devices will be located, what the devices look like, and any potential issues that may arise. Training is also important for the personnel reviewing access reports or other such data, so they understand any new terminology or data elements in reports.

4.7 Legal Considerations

As airports consider the use of biometrics in connection with their access control systems, legal considerations are frequently viewed as impediments. In most cases, careful analysis of the existing legal requirements and careful planning around privacy considerations can mitigate these concerns. Most airports that have embarked on biometric programs indicated that consultation with airport legal staff is an important part of the planning process.

In addition to general privacy concerns around the use of biometrics, airport stakeholders whose employees will be utilizing the access control programs may need to address labor and bargaining concerns with their employees. This may require restrictions on the use of the biometric data from the access control system. Limitations on the use of access control data in connection with employee access or minor disciplinary matters are commonplace restrictions.

Conducting a PIA following the model offered by DHS or application of NIST Privacy Framework analysis as part of the planning process could facilitate legal analysis and assist in building a system that complies with both current legal norms and developing legal trends. Section 6.2.3 outlines FIPPs that DHS has adopted for use in their privacy policy for PII. The discussion below outlines how these may apply to airports implementing biometrics for access control.

- **Transparency:** This measure works with the concepts of informed notice and consent to strengthen user confidence in the biometric systems.
- **Purpose Specification:** A statement of purpose such as "Biometric enhancement of access security restricts access by unauthorized personnel in accordance with federal requirements" would be an acceptable purpose statement for biometric access control. Multiple purposes can be included in a specification of purpose, but it may expand the concerns that stakeholders have regarding biometric data collection.
- **Use Limitation:** Use of biometric data must be in strict accordance with the stated purpose for which the data is collected. It is bad practice to expand use of data beyond the stated purpose, such as for monitoring employee time or performance.
- **Data Minimization:** Implement data collection and retention practices that are narrowly tailored to the stated purpose. When an individual's biometric data is no longer needed for access control system use, it is best practice to eliminate the person's the data from the database.

  If utilizing smart cards, the airport may only store the fingerprint template on the ID media issued to the individual. Additionally, airports need to be mindful of legal requirements that might be inconsistent with operational requirements or best practices for data retention.
- **Individual Participation:** Individuals utilizing the biometric access control system need to understand specifically what biometric is going to be collected and how it will be used. Airports already do this for fingerprints collected in the credentialing process for Criminal History Records Checks (CHRC), which includes execution of a detailed Privacy Act Notice and consent forms. However, the collection of biometrics for use in access control is not the same as the CHRC process, and the airport should conduct a separate process for notice and consent when collecting biometrics for use with access control systems.
- **Security:** Airports need to safeguard biometric data. Security of this data and the responsibilities that may be imposed by state or local regulation in the event of a breach require policy consideration and response planning.
- **Data Quality and Integrity:** Airports utilizing biometric measures should ensure that biometric data is properly encoded into access control systems and ID media. This process should include validating identity, and ensuring that aviation workers are correctly enrolled and able to utilize the access control systems.
- **Accountability and Auditing:** Processes for accountability and auditing the biometric systems ensure that they are operating properly and in accordance with design and policy. This is essential for achieving compliance with legal standards and for limiting liability. Additionally, properly executed audits provide evidence of compliance, which can be used to counter allegations of system misuse.

Additionally, deploying biometric access control requires compliance with various legal and regulatory frameworks, including data protection, privacy, and employment laws. Ensuring adherence to relevant regulations and obtaining necessary approvals or consent is vital.

SECTION 5: IMPLEMENTING BIOMETRICS IN THE PASSENGER JOURNEY

While implementing passenger processing procedures is the responsibility of air carriers and federal agencies, the deployment of those solutions in airports has implications for a wide array of facility and operational decisions. Facilities and processes must be adapted as tenant organizations adjust their infrastructure and organizational practices to facilitate touchless processing. Passenger screening checkpoints may also require changes to accommodate new processes. Numerous considerations should be taken into account, as listed below and in the following sections. There are many similarities to the considerations for access control.

5.1 Needs Assessment and Requirements Development

Needs assessments for biometrics in the passenger journey are similar to those for access control deployments:

- Align planning and implementation to address both airport and airline business objectives.
- Perform a baseline study of existing processes to measure improvement. Consider introducing behavioral science in addition to industrial engineering to assess biometric processes.
- Increased efficiency is an important goal but may not be the most important objective. There are other considerations as to why an airport may look at biometrics, including security enhancement, user acceptance, regulatory/compliance, and reputation.
- Enlist extensive stakeholder involvement in planning and implementation. It is important to have early buy in and understanding from all airport stakeholders.
- Conduct in-depth research on biometric solutions before implementation.
- Identify the specific points in the passenger journey where biometric verification will be used. This may include self-service check-in kiosks, security checkpoints, boarding gates, and immigration control. Determine the necessary infrastructure and equipment required at each point.

5.2 Selection Criteria

With respect to checkpoint operations, TSA purchases, maintains, and operates the biometric screening equipment. The airport has no role in the selection of devices for processing at security checkpoints operated by the TSA.

For biometric systems used in connection with boarding or bag drop, the role of the airport in device selection will depend on whether the system is a proprietary airline system or a common-use system. The airport will likely have no role in device selection for proprietary systems. If the system is common use, the airport will have overall responsibility for selection of the device (hardware and software). However, the device selections must meet the specifications set out by the federal entities responsible for supervising the function (i.e., TSA for bag checks and CBP for domestic boarding on international flights). Those devices must also integrate with any airport common-use platforms accessible to the air carriers for their passenger processing.

The selection criteria and product review and testing concepts discussed for biometric access control (see Sections 4.2 and 4.3) may also apply to biometric systems implemented for passenger use.

5.3 Technology and Integrations

Consider industry standards and interoperability requirements to enable seamless integration with other airports, airlines, and CBP. Align with common protocols and formats to facilitate interoperability and promote a consistent experience for passengers.

The integration of biometrics into the passenger journey is dictated largely by the biometrics prescribed by CBP and TSA for passenger processing. Currently, facial recognition is used by TSA and CBP, and iris and fingerprint technologies are used for the CLEAR Registered Traveler program.

Airlines are also adopting facial recognition for their bag-drop processes and for use at boarding gates. Some airlines have developed digital ID applications for use in lieu of providing drivers' licenses and other forms of government identification.

Airline integration with software and hardware supporting passenger processing will require an amendment to their aircraft operator security plan. This will require TSA certification for every airline using a common-use system. As requirements change across airports that may use different hardware and software combinations for biometric processing, the airlines will be required to amend their regulated security plans for each separate airport. The challenge of differing integrations at multiple airports leaves some air carriers with a strong preference against a common-use approach for biometric processing.

Depending on how TSA proceeds with its biometric implementations, airports may also need to respond to requirements for reconfiguration or adaptation of passenger screening checkpoints.

5.4 Deployment

Stakeholders in biometric planning and implementation for the passenger journey commonly include:

- Facilities and operations personnel
- IT services personnel
- Legal services personnel
- Airport customer service and airline relations personnel
- Air carriers
- Consultants and integrators
- Hardware and software vendors
- Governmental entities (CBP and TSA)

Airports with more expansive personnel also have services provided by airport innovation teams, industrial engineers, and data scientists.

Air carrier personnel involved in the process of planning and implementing passenger journey solutions include facilities, real estate, legal operations, IT services, and customer service personnel.

In instances where the project is common use, the vendors and consultants are retained by the airport, although it is not unusual to also have consultants retained by the air carrier. In proprietary airline systems, the consultants and vendors are retained by the airline.

For the passenger journey, passengers must opt in to the biometric system. In the case studies, airlines posted information on websites and other locations to encourage passengers to use the system, as well as customer service contact information to report or get assistance with issues.

Deployment of passenger biometric systems should include an education and awareness campaign to inform passengers about the biometric system, its benefits, and how their data will be used and protected. This campaign should include clear communication channels to address passenger inquiries or concerns. Outreach through travel advisories may also be considered to ensure passengers are aware of the new systems and processes.

Establish a user-friendly and efficient process for enrolling passengers into the biometric system. Consider factors like enrollment location (e.g., dedicated kiosks or mobile devices), trained personnel, enrollment time, and privacy considerations. Be able to provide clear instructions and assistance to passengers during the enrollment process.

Airports may consider setting up demonstration stations where passengers can test the system prior to reaching the security screening checkpoint to increase familiarity with the processes. Instructional signage may also be used to aid passengers through the process.

Comprehensive training should be provided to airport staff who are involved in passenger handling to ensure they are proficient in using and troubleshooting the biometric system. Open lines of communication should be maintained with staff to address any concerns, feedback, or questions related to the system.

5.5 Legal Considerations

One of the principal impediments to the adoption of biometric technologies for the passenger journey is concern over legal restrictions. Unlike the collection of biometrics for access control purposes, which involves a narrow and defined group of persons who have a working relationship with the airport, the passenger journey process involves a transient population with a narrow time for use of the data collected. Additionally, the use of biometric data in connection with a commercial process like passenger travel invokes a different body of law than applies to employees or invitees. The growing development of legal protections for consumers at both the state and federal level is an important consideration with respect to use of biometrics for passenger processing.

In cases where biometrics are required for federally specified processes, like the CBP's exit program and the use of TVS, the legal path is clear. Use permissions and requirements around collection and retention of biometric data used for TVS processing are narrow and strictly controlled. Airports and airlines collecting data for TVS processing are obligated to comply with TVS requirements. In cases where the airports or airlines are looking to collect and utilize biometrics in connection with domestic travel or for processes like bag check or security processing, which are not part of a federally specified process, the legal environment is more uncertain.

The legal environment for TSA biometric checks at passenger screening checkpoints or in connection with bag checks will likely not be clear until those processes mature. Given that TSA has indicated intent to utilize the TVS in connection with its identity management systems, it is likely that TSA-mandated processes will require compliance with TVS rules. This would result in limited use and/or retention of collected biometric data. However, it should be noted that the ability of TSA to use TVS lacks the direct statutory authority afforded to CBP. TSA use of TVS has been the subject of criticism by advocacy groups and some members of congress.

To avoid legal concerns over biometric data, airports may wish to consider supporting digital identity solutions. These systems eliminate the need for airlines or airports to directly collect or store biometric data. The passengers have the biometric verification data stored on their phones and make the determinations as to when and with whom that information is shared.

When an airport undertakes to involve itself in the collection of passenger data (usually through operation of common-use systems for baggage check in or e-gate management), it needs to ensure compliance with legal requirements around the collection and use of that data. Where those systems are operated in a proprietary fashion by airlines, the airport is generally not involved in data collection. Where the airport is involved as a common-use system operator of a system that is collecting biometric information, or if the airport otherwise receives biometric information from airlines involved in passenger processing, consultation with legal counsel is advised.

When dealing with passenger data, the airport should always ensure compliance with applicable privacy regulations and obtain necessary consent from passengers. Prioritize the privacy and data protection of passenger biometric data, and implement strong security measures to protect the data throughout its life cycle, including encryption, access controls, and monitoring mechanisms.

The FIPPs applied to biometric access control (Section 4.7) is a good starting point to assess and mitigate potential liability. While many of the considerations will be the same as for access control, the focus for each consideration will be different.

- **Purpose Specification:** The current rules imposed by CBP restrict the use of biometric data for purposes other than TVS processing. Where airports or airlines request permission from CBP to utilize biometric data for other purposes, those uses need to be clearly specified and determined to be consistent with DHS/CBP’s limitations.
- **Use Limitation:** Use of biometric data must be in strict accordance with the stated purpose for which it is collected. Use beyond a stated purpose may expose airports or airlines to liability under state or federal consumer protection laws. Moreover, the collection and use of data outside the stated purpose may undercut passenger confidence in the processing systems.
- **Data Minimization:** The airport should consider developing collection and retention practices that are narrowly tailored to the stated purpose. In this regard, the use of digital ID applications greatly reduces the exposure of airports and airlines, as the digital images and templates can be utilized to confirm identity without the need for the airport or airline to retain biometric data. These measures would enable airports to minimize exposure for retained data as well as maximize passenger control over their individual data.
- **Individual Participation:** Individuals utilizing biometric passenger processing need to be provided with clear notice and must give consent to their participation. The ability to opt out of biometric processing should also be clearly stated. Airports should consult with their counsel in the creation of notice and consent forms, both written and electronic, as well as signage advising passengers of their option to participate.

  Opt-out measures are currently mandated by CBP for US citizens. The CBP requires posting of specifically worded opt-out signage and airport/airline capability to process passengers who exercise their right to opt out. These legal requirements for notice and consent and the ability to opt out have clear operational and facility implications.
- **Security:** The introduction of biometrics in the passenger journey will expand the sensitivity of the data collected in this process. This needs to be accounted for with respect to data security measures as well as the process to authenticate identity, which will often occur in public areas utilizing kiosks or via third-party applications on mobile phones. This may require physical and

virtual security measures such as physical queue spacing at airports and security measures like encryption. Applying these measures has legal implications for maintaining security and defending data collection practices.

- **Data Quality and Integrity:** Because the process of passenger biometric enrollment occurs in a time constrained and public environment, and often through self-service applications, ensuring data quality can be challenging. Airports or airlines collecting the data will bear legal responsibility for ensuring the fidelity of that data.
- **Accountability and Auditing:** Robust auditing systems to ensure accountability and proper system function are key measures to mitigate against system misuse or malfunction. An audit may need to be performed by a governmental entity such as TSA or CBP to ensure that data collection practices are in accordance with TSA and/or CBP requirements and not being improperly collected or retained. Airports involved in biometric data collection for passenger processing need to understand the audit process and ensure they are being applied. There also needs to be mechanisms in place for the airport to access audit findings so that corrections can be made to any errant system.
- **Transparency:** Passenger understanding of biometric data collection practices and use of data have real legal implications in the area of commercial transactions. Hidden collection or use practices can potentially lead to liability as deceptive or unfair consumer practices. These concerns can be mitigated by implementing clear and unambiguous polices around biometric collection and use. The airport should ensure that all partners, such as airlines and application developers, adhere to the published practices around the collection and use of biometrics.

  Where an airport determines to collect and utilize anonymized data in connection with a system gathering biometric data (e.g., numbers of individuals processing, processing times), it might consider disclosing that fact to the system users to guard against potential liability claims.

Answering questions about compliance with the legal considerations outlined above requires a detailed analysis linked to the specific jurisdiction in which the airport is located. It is important to engage legal counsel to help guide the airport in addressing these considerations.

SECTION 6: LEGAL AND POLICY CONSIDERATIONS

The legal and policy environments present a host of considerations with respect to the implementation of biometric solutions for both access control and passenger processing. In many instances, it is concern over legal issues that inhibits airports from greater use of biometrics. Understanding these issues will help airports make better decisions about the use of biometric technologies.

The development of biometric solutions both for access control and in connection with the passenger journey are not without controversy. Privacy and civil liberties concerns have been raised by several advocacy groups,[44] and some state laws and local ordinances have served to limit use of biometrics.[45] Even at the federal level, there have been proposed moratoriums on the use of biometrics.[46] Understanding and respecting privacy requirements are hallmarks of the guidance on development of biometric programs.[47]

6.1 Legal and Regulatory Trends

Privacy protections in the US can best be described as a patchwork quilt. Unlike countries such as Canada or those in the European Union, the US does not have any centralized body of privacy law, but instead tends to apply what is called a sectoral approach. Some sectors, like healthcare and finance, have greater privacy protections than others. In addition to being more sectoral focused, privacy protections are characterized by varying state and local regulatory schemes. A detailed summary of federal, state, and local protections for privacy can be found in ACRP Legal Research Digest 42, "Legal Implications of Data Collection at Airports" (ACRP LRD 42).[48] A shorter summary of those protections can be also found in the NAS publication "Airport Biometrics: A Primer" (Biometric Primer).[49]

6.2 Federal Legal Provisions

The federal protections specifically addressing biometrics are limited. There are US Supreme Court cases that generally address protections against compelled government collection of biometrics[50] and government use of private information for purpose of tracking the movements of individuals.[51] In both

[44] See, e.g., Marc Rotenberg, et. al., "Letter to The Honorable Bennie Thompson, Chairman The Honorable Mike Rogers, Ranking Member Committee on Homeland Security U.S. House of Representatives," (February 5, 2020) Cited at https://epic.org/documents/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies-part-ii.

[45] National Academies of Sciences, Engineering, and Medicine. Legal Implications of Data Collection at Airports. Washington, DC: The National Academies Press, 2021 pp. 49–51. Cited at https://doi.org/10.17226/26207.

[46] See e.g., Hon Jeffery Merkley, et al. February 9, 2023. "Letter to Administrator David Pekoske" Cited at TSA Facial Recognition Technology letter (politicopro.com) (Correspondence from five U.S. Senators seeking a moratorium on TSA and CBP biometric programs).

[47] Transportation Security Administration 2018. "TSA Biometric Roadmap, For Aviation Security & the Passenger Experience" p.18. Cited https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[48] National Academies of Sciences, Engineering, and Medicine. *Legal Implications of Data Collection at Airports*. Washington, DC: The National Academies Press, 2021. Cited at https://doi.org/10.17226/26207.

[49] National Academies of Sciences, Engineering, and Medicine 2021. "Airport Biometrics: A Primer." Washington, DC: The National Academies Press. Cited at https://doi.org/10.17226/26180.

[50] See, e.g., King v. Maryland, 569 U.S. 435 (2013) (holding that individual privacy interests in biometric DNA samples by persons charged with or convicted of serious crimes were overridden by compelling governmental interests).

[51] See, e.g., Carpenter v. U.S. ___ U.S. ____, 138 S.Ct. 2206 (2018) (holding that individual privacy interest in cell site location information allowing for the tracking of location over an extended period of time required the government to obtain a warrant before accessing the information).

cases, the court held that under certain circumstances privacy protections would limit government access to information in which an individual has a constitutionally recognizable privacy interest. These cases are important because they establish that some privacy interests, including interests in biometric information, are afforded protections under the US Constitution. The contours of those protections are not entirely clear. Moreover, nothing suggests these constitutional protections extend to biometric or other personal information that is voluntarily provided.

Just as the parameters of constitutional protections are unclear, there is no comprehensive federal statute addressing government use of biometrics.[52] However, as the use of biometrics has increased, some congressional efforts are being made to create legislation that limits or places a moratorium on the use of biometrics. As is noted in ACRP LRD 42 and the Biometric Primer, under the federal sectoral approach privacy protection is limited to certain uses by certain users, both public and private, in differing contexts. With respect to protection of biometric use for access control or passenger processing, the statutes discussed in Sections 6.2.1 and 6.2.2 and their enforcing regulatory provisions are of particular interest. The legal restrictions around the collection and use of biometric information in connection with issuance of airport credentials demonstrates how two federal statutory provisions work to address privacy concerns.

6.2.1 Federal Protections for Certain Criminal Justice Information

The collection and use of biometrics in connection with law enforcement–related operations has been long accepted under federal law. The Department of Justice (DoJ) through the FBI has managed fingerprint operations since the 1920s. The FBI's Integrated Automated Fingerprint Information System was established in the late 1990s.[53] The automated fingerprint repository operated by the FBI is now called Next Generation Identification (NGI).[54] NGI also includes the FBIs Interstate Photo System, which supports facial recognition search capabilities for over 30 million mugshots.[55]

The provisions of 28 United States Code (USC) § 534 permit the DoJ to collect fingerprint information and disseminate it for authorized purposes. The process for use of information from the NGI system is regulated under 28 CFR Part 20 that manages establishment and use of the federal Criminal Justice information system, which is managed by the FBI's Criminal Justice Information Services (CJIS) division.

Criminal History Record Information (CHRI) is linked to the biometric fingerprint information in NGI through the Interstate Identification Index. In accordance with regulations, CHRI is considered sensitive, but unclassified. In a 1989 ruling, the US Supreme Court concluded that individual privacy concerns left those records protected from disclosure requirements under the federal Freedom of Information Act (5 USC, § 552 et. seq.). While access to CHRI was initially exclusively limited to law enforcement

[52] See, e.g., "Facial Recognition and Biometric Technology Moratorium Act of 2021" S 2052, 117th Congress (2021) cited at https://www.congress.gov/bill/117th-congress/senate-bill/2052.

[53] Federal Bureau of Investigation, "Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling" (May5,2008). Cited at https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments/firs-iafis.

[54] Federal Bureau of Investigation, "Next Generation Identification (NGI)" FBI Website, cited at https://le.fbi.gov/science-and-lab-resources/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi#:~:text=The%20Next%20Generation%20Identification%20(NGI)%20Iris%20Service%2C%20provides%20a,repository%20within%20the%20NGI%20system.

[55] Ibid.

purposes, that access has been expanded to support other purposes such as employment suitability determination through a system of authorized private contract channelers.

One of the federal initiatives authorized for access to CJIS information for non-criminal justice purposes are fingerprint-based CHRCs, referenced in 49 CFR § 1542.209, which are used by airports in connection with credentialing processes. The regulations requiring the collection and submission of fingerprints place limits on the use and dissemination of CHRI received in response to requests submitted through channelers. These limits are imposed on airports and air carriers though TSA-supervised regulations and contracts with the channelers.

6.2.2 Federal Privacy Act of 1974

In addition to the CJIS requirements imposed on airport operators and air carriers in conjunction with credential issuance in 49 CFR § 1542, there are also restrictions imposed on the federal government itself. The Privacy Act of 1974 (USC, § 552a et. seq.; the "Federal Privacy Act") governs use of information, including PII collected or received by the federal government. Provisions of the Federal Privacy Act include a range of privacy protections, including requirements for providing notice and consent around data collections, restrictions on use and dissemination of information, requirements for safeguarding information, requirements for individual access and redress, and provisions for auditing.

To effectuate the provisions of the Federal Privacy Act with respect to background vetting for the credentialing process, TSA requires airports to provide first time and renewal applicants with a Privacy Act Notice. The notice outlines the federal government's use of biometric and other PII provided for vetting. It includes notice that the information provided will be shared with and retained by other agencies like the FBI.

While the Federal Privacy Act only applies to information in the possession of the federal government, the protections and practices found in the Federal Privacy Act have been copied and adopted by states and other entities.

6.2.3 Fair Information Practice Principles

In contrast to the well-established provisions concerning the collection of biometric data in connection with airports vetting aviation workers, there is little in the way of direct legal guidance for collection of biometric information for passenger processing. Federal Privacy Act provisions do not apply to air carriers or airports collecting that information.

Given the commercial nature of passenger processing transactions, the Federal Trade Commission (FTC) may have some authority over the process. The FTC regulates actions of parties that may affect competition in the marketplace through Section 5 of the Federal Trade Commission Act[56] and provides protections against "unfair or deceptive acts or practices in or affecting commerce." Through this authority, the agency has taken many enforcement actions to protect privacy, including actions against improper or unauthorized use of information provided by consumers, or where reasonable data security practices are not followed.[57]

[56] 15 USC § 45(a).

[57] See, e.g., Federal Trade Commission, "FTC Report to Congress on Privacy and Security" (Feb. 2020). Cited at https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

One of the FTC's primary strategies concerning data privacy and security is promotion of the Fair Information Practice Principles (FIPP), which have influenced much of the current thought about privacy and data protection in the US and globally.[58] In their "Privacy Policy Guidance Memorandum," DHS formally adopted the following FIPPs in the policy for use of PII: [59]

- **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of 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.

In its most recent publication on the issue of identity management for both aviation worker vetting and passenger processing, the TSA noted its commitment to the application of FIPPs. The *TSA Identity Management Roadmap* indicates:

> DHS's Fair Information Practice Principles regarding transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing will inform TSA's privacy considerations. These principles will

[58] See Privacy Online: Report to Congress, F.T.C. (1998), at 48, n. 27, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[59] U.S. Department of Homeland Security Privacy Office, "Privacy Policy Guidance Memorandum" DHS Privacy Office Memorandum Number 2008-01 (December 28, 2008) pp. 3-4. Cited at https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf. (This Privacy Guidance was reaffirmed in 2017 by U.S. Department of Homeland Security Privacy Office, "Privacy Policy Guidance Memorandum" DHS Privacy Office Memorandum Number 2017-01 (April 25, 2017). Cited at https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

> continue to guide TSA as it seeks to protect privacy while enhancing proofing, enrollment, and vetting technology, and improving the passenger experience.[60]

The GAO's 2020 review of the CBP's collection and use of biometric data notes that CBP is applying FIPPs principles and uses the FIPPs analysis to evaluate its own efforts to protect privacy.[61] Both the TSA's CAT program[62] and the CBP TVS program[63] have been the subject of agency-conducted PIAs to assess program compliance with FIPPs requirements.

While FIPPs may not have the full effect of legal requirements for airports and air carriers, governmental entities such as TSA and CBP will be required to follow FIPPs in their involvement in biometric processing for passenger journeys. FIPPs would also likely influence TSA's regulatory judgments with respect to airport access control programs. Considering these factors, it would be advisable for airport operators and air carriers to acquaint themselves with FIPPs. Airports and air carriers thinking of adopting biometric solutions should consider adopting FIPPs as the guiding principles for their biometrics governance strategy.

6.3 State Legal Provisions

This section provides examples of state legal measures that address biometrics both specifically and as part of larger statutory regimes that regulate PII. This can serve as a starting point for review and evaluation by airport operators and their counsel. ACRP LRD 42 also summarizes state legal provisions concerning biometric use in airports.[64]

6.3.1 State Privacy Acts

PUBLIC SECTOR OPERATIONS

There are a limited number of state laws that directly address biometric collection and use. Most states have laws that generally apply to biometrics as part of PII collection and use. These include laws in all fifty states addressing government collection and use of PII data.[65] Many of these laws are modeled after the provisions of the Federal Privacy Act. Accordingly, the application of FIPPs offers a good starting point for compliance (see Section 6.2.3). Many of these laws apply not only to state government operations, but also to the operations of counties, municipalities, and other public entities. Airport operators are advised to work with airport counsel to understand the applicability and implications of

[60] Transportation Security Administration 2022. "TSA Identity Management Roadmap," Washington D.C. at P. 28. Cited at https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf.

[61] General Accountability Office 2020. "Facial Recognition, CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues" GAO Report 20-568 (September 2020) pp. 37-38. Cited at https://www.gao.gov/assets/gao-20-568.pdf.

[62] Transportation Security Administration, "Travel Document Checker Automation-Digital Identity Technology Pilots" Privacy Impact Assessment, DHS/TSA/PIA 51 (January 14, 2022). Cited at https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-tsa051-digitalidentitytechnologypilots-january2022_0.pdf.

[63] Customs and Border Protection, "Travel Verification System" Privacy Impact Assessment DHS/CBP/PIA-56.Cited at (November 14, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[64] National Academies of Sciences, Engineering, and Medicine. *Legal Implications of Data Collection at Airports*. Washington, DC: The National Academies Press, 2021. Cited at https://doi.org/10.17226/26207.

[65] National Conference of State Legislatures "Data Security Laws: State Government," National Conference of State Legislatures (Feb. 14, 2020). Cited at https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx.

state privacy acts to their operations. The National Conference of State Legislatures (NCSL) offers a publicly accessible collection of those statutes.[66]

PRIVATE SECTOR OPERATIONS

Some general provisions under state law place requirements around private sector PII data collection and use. In some instances, this can include biometric information. These measures were in effect in half the states as of May 2019.[67] These statutes principally focus on ensuring that entities collecting and retaining PII data use "reasonable security procedures and practices." While these practices only apply to private sector parties and not governmental entities, they may apply to stakeholders like air carriers. As with privacy acts applying to government activity, these statutes should be reviewed with airport counsel to assess applicability. The NCSL website is a good resource to identify these statutes.

6.3.2 State Breach Notification Laws

The unauthorized release of PII, whether through inadvertent or intentional misconduct of employees or through external forces, creates significant security and liability risk. All fifty states now have breach notification laws that specify requirements for breach of security procedures resulting in unauthorized access to PII. These statutes cover biometric information where it is included in the statute's definition of PII. The laws in some states focus solely on private entities, while others also apply to governmental entities. These laws include provisions addressing parties that must comply and definitions of critical terms like PII and breach, and establish parameters of notice (who, when, and how). The NCSL maintains a reference index of state security breach notification laws.[68] Given the potential costs that could be imposed in the event of breach, understanding the applicability of these laws should be discussed with legal counsel.

Airports should work with their counsel to review their breach planning, mitigation, and response policies and procedures. Those policies and procedures will require interdisciplinary efforts to be successful. Conducting tabletops and exercises to test those plans should be considered.

6.3.3 State Data Disposal / Destruction Laws

Good data security planning includes ensuring PII data that is no longer required for retention is disposed of, destroyed, or otherwise deleted from records. In 2019, the NCSL reported the existence of data disposal laws in thirty-five states and in Puerto Rico.[69] These laws frequently apply to both governmental and private organizations. The laws are in addition to the FTC's Disposal Rules for consumer-related PII data.[70] Airport operators need to work with their counsel to ensure practices for data disposal or destruction comply with both state and FTC requirements.

[66] Ibid.

[67] National Conference of State Legislatures "Data Security Laws: Private Sector", Official Website Nat'l Conf. of State Legis. (May 29, 2019), Cited at https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws.

[68] National Conference of State Legislatures, "Security Breach Notification Laws," Official Website Nat'l Conf. of State Legis. (July 17, 2020). Cited at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[69] National Conference of State Legislatures, "Data Disposal Laws," Official Website Nat'l Conf. of State Legis. (Jan. 4, 2019). Cited at https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[70] Federal Trade Commission "Disposing of Consumer Report Information? Rule Tells How," FTC (June 2005). Cited at https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how.

6.3.4 State Consumer Privacy Laws

California,[71] Colorado,[72] Connecticut,[73] Utah,[74] and Virginia[75] have created consumer protection laws that may address biometric information along with other PII provided in connection with commercial transactions. These statutes apply several data protection concepts, including those identified in the FIPPs. Many of these statutes did not become effective until 2023, so their effect has not yet been fully felt.

Statutes specifically focused on the collection and use of biometric are found in Illinois,[76] Texas,[77] and Washington.[78] These statutes are explored in greater detail in ACRP LRD 42.[79] The most comprehensive of the three is the Illinois Biometric Information Privacy Act (BIPA),[80] which was enacted in 2008 and provides detailed provisions regarding collection, retention, use/disclosure, and destruction of biometric information.[81]

BIPA imposes three requirements on entities collecting biometric information: (1) the subject must be advised of the biometric being collected or stored; (2) the subject must be advised in writing of the purpose of collection and use, and the length of time the biometric information will stored and used; and (3) the subject must provide a written release.[82] BIPA also provides for civil remedies for persons whose biometric information was taken or used in a matter inconsistent with the statutory requirements. The remedies include statutory damages and attorney's fees for a prevailing party.[83] As a result, it has generated substantial litigation, settlements, and potential damage awards.[84]

The research did not provide any examples of misuse of biometric data at airports. However, there are examples under Illinois BIPA where use of biometric information was inconsistent with the statutory provisions of the requirements for collection and use of biometric data. Often the violations involved failing to comply with notice and consent requirements in the collection of biometric data, or failing to

[71] "California Consumer Privacy Act of 2018," Civil Code Division 3, Part 4, Title 1.81.5. Cited at Codes Display Text (ca.gov); amended by the "California Privacy Right Act (2020)" Cited at https://transcend.io/laws/cpra/#section-1.

[72] "Colorado Privacy Act," Colorado Revised Statutes, Part 13, Sec. 6-1-1301 (eff. July 1, 2023) cited at Colorado Revised Statutes | Part 13 - [Effective 7/1/2023] COLORADO PRIVACY ACT | Casetext.

[73] "An Act Concerning Personal Data Privacy and Online Monitoring," Connecticut Public Act 22-15 (eff. July 1, 2023). Cited at AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

[74] "Utah Consumer Privacy Act," Utah Code Annotated, 13-61-101.

[75] Consumer Data Protections Act," Code of Virginia, Chapter 53, Section 59.1-575 et. seq. (eff. January 1, 2023). Cited at § 59.1-575. (Effective January 1, 2023) Definitions (virginia.gov).

[76] Biometric Information Privacy Act, 740 ILCS 14/1 et seq. Cited at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[77] Tex. Bus. & Com. Code Ch. 503. Cited at https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

[78] Wash. Rev. Code Ch. 19.375. Cited at https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true#:~:text=(1)%20A%20person%20may%20not,identifier%20for%20a%20commercial%20purpose.

[79] National Academies of Sciences, Engineering, and Medicine. *Legal Implications of Data Collection at Airports*. Washington, DC: The National Academies Press, 2021. Cited at https://doi.org/10.17226/26207.

[80] Biometric Information Privacy Act, 740 ILCS 14/1 et seq. Cited at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[81] 740 ILCS 14/15.

[82] 740 ILCS 14/15(1)-(3).

[83] 740 ILCS 14/20.

[84] See, e.g. In re Facebook Biometric Information Privacy Litigation, 522 F. Supp. 3d 617 (N.D. Cal. 2021) (District Court approval of $650 million class action settlement for Facebook use of facial images); and Cothron v. White Castle Systems, Inc., 2023 IL 128004 (Feb. 17, 2023) (Illinois Supreme Court concluded that every swipe of fingerprint biometric obtained in violation of BIPA was potentially actionable for $1000 or $5000 depending on intent. A potential judgement that the dissent characterized a s potentially "annihilative Liability" for the company).

destroy collected biometric data once the purpose of collection was completed. Examples include a fast food company that failed to comply with consent requirements when gathering and using biometric data for employees to access their payroll records,[85] and an amusement park that collected fingerprint data without meeting the statutory requirements for consent for use in customer access to the amusement park.[86] The amusement park company also continued to maintain the biometric data after the access rights to the amusement park expired. This case was settled for $36 million.[87]

While an airport's home state may not specifically regulate biometric data collection and use, the above examples demonstrate that misuse of biometric information may have substantial consequences. Airport counsel should review current laws to ascertain any developments relative to biometric collection use, storage, or destruction.

6.3.5 Local Ordinances Regulating Facial Recognition Biometric Use

From 2019 to 2021, a spate of local governments and governmental entities sought to place a moratorium on government use of facial recognition biometric technology. In 2019, these included San Francisco;[88] Oakland, California;[89] Somerville, Massachusetts;[90] and the Port of Seattle Commission regarding Seattle-Tacoma International Airport.[91] In 2020, moratoriums were enacted in Boston[92] and Portland.[93] Baltimore[94] and Pittsburgh followed in 2021.

Most of the ordinances focused on policing operations. In one case, the ordinance excepted access control uses for facial recognition. However, most of these types of ordinances make the use of facial biometrics in access control more difficult if not impossible to implement.

These types of ordinances offer examples for airports of local concerns that can limit access to security tools. They also demonstrate an unsettled legal environment over government use of facial recognition, and offer a caution for airport operators looking to adopt facial recognition.

[85] Cothron v. White Castle System Inc. cited at https://law.justia.com/cases/illinois/supreme-court/2023/128004.html

[86] Rosenbach v. Six Flags Entertainment Corp. cite at https://law.justia.com/cases/illinois/supreme-court/2019/123186.html

[87] https://www.lexology.com/library/detail.aspx?g=5faf2de4-956c-45bb-a361-cbc9a6c2372f

[88] S.F. Admin. Code Ch. 19B. Cited at https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320

[89] Oakland Mun. Code 9.64. Cited at https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE_9.64.045PRACUSBISUTEPRPOTE#:~:text=A%20summary%20of%20community%20complaints,subject%20to%20the%20technology's%20use.

[90] Somerville Ord. No. 2019-16, § 9-25. Cited at https://library.municode.com/ma/somerville/ordinances/code_of_ordinances?nodeId=966223.

[91] Motion 2019-13, A Motion of the Port of Seattle Commission, Port of Seattle Commission Meeting (Dec. 10, 2019). Cited at https://www.portseattle.org/sites/default/files/2019-12/Motion%202019-13__Biometrics%20Principles.pdf.

[92] Bos. Ord. No. 16-62. Cited at https://www.universalhub.com/files/recognitionban.pdf.

[93] City of Portland, "City Council Approves Ordinances Banning Use of Facial Recognition Technologies by City of Portland Bureaus and By Private Entities in Public Spaces," (Sept. 9, 2020) Cited at https://static1.squarespace.com/static/5967c18bff7c50a0244ff42c/t/5f3ad787ba3fd27776e444af/1597691785249/Ordinance+to+ban+use+of+FRT+in+Places+of+Public+Accommodation+plus+code+amendment+-Final.pdf.

[94] Baltimore Enacts Facial Recognition Moratorium" Cited at https://content.next.westlaw.com/practical-law/document/Id323c80ece9811ebbea4f0dc9fb69570/Baltimore-Enacts-Facial-Recognition-Moratorium?viewType=FullText&transitionType=Default&contextData=(sc.Default).

6.4 Accommodating Persons with Disabilities

An outline of legal standards regarding an airport's obligations to provide accommodations for persons with disabilities is found in the FAA Advisory Circular "Access to Airports by Individuals with Disabilities."[95] FAA also maintains a website with resources to assist airports in meeting disability compliance.[96]

When designing programs for introduction into the passenger journey process, airports should engage experts in ADA compliance, including legal professionals, architects, and engineers, to ensure that improvements in facilities and systems meet those requirements.

6.5 Privacy Frameworks

Airports moving to incorporate biometrics into the passenger journey and access control is reflective of larger societal trends to adopt that technology. At the same time, biometric collection and use is the subject of growing privacy concerns. This is particularly the case for facial biometrics. In 2020, the GAO issued a report examining both the market development and maturity of privacy protections for facial biometrics.[97]

The GAO report noted little in the way of enforceable legal and regulatory controls over commercial use of biometrics in the US. It concluded that in the absence of enforceable legal requirements, US users could look to the application of nationally and internationally promulgated standards to regulate biometric use. Models like the European Union's efforts under the General Data Protection Regulation[98] and NIST's Privacy Framework[99] were offered as examples.

The existence of larger national and international efforts to integrate biometric technology into a range of commercial and private uses offers airport operators a wide range of examples for the application of biometrics. It also offers examples of government strategies and policies to protect privacy and civil rights in conjunction with biometric use.

As airports consider the use of biometrics, it may offer an opportunity to strengthen privacy protections that govern collection of all PII. The heightened sensitivity of biometrics may increase the concerns of stakeholders in the robustness of those programs.

The protection of biometric data is best accomplished through a comprehensive data privacy protection plan. The NIST Privacy Framework can help airports to establish a complete program to ensure that privacy is managed. A framework such as NIST's provides airports with a roadmap to achieve the goals of their privacy policies and afford data security.

[95] Federal Aviation Administration, "Access to Airports by Individuals with Disabilities," Advisory Circular, No: 150/5360-14A (December 6, 2017). Cited at https://www.faa.gov/documentLibrary/media/Advisory_Circular/150-5360-14A.pdf.

[96] Federal Aviation Administration, Office of Civil Rights," Airport Disability Compliance Program (ADCP)" FAA Website. Cited at https://www.faa.gov/about/office_org/headquarters_offices/acr/com_civ_support/disability_compliance.

[97] General Accountability Office 2020. "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses," *GAO 20-522*. Washington D.C. Cited at GAO-20-522, Facial Recognitions Technology: Privacy and Accuracy Issues Related to Commercial Uses.

[98] Gen. Data Protection Reg., 2016/679 (EU). Cited at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[99] U.S. Department of Commerce, National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management," Version 1.0, (January 16, 2020). Cited at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

As part of a comprehensive approach to privacy, airports should also consider adopting Privacy by Design (PbD) principles.[100] PbD works to weave privacy protection into the fabric of organizational processes. It includes technical, operational, and administrative considerations, and encourages a proactive and transparent system that addresses privacy protection as a positive value in meeting organizational goals and objectives. The system of protection centers around ensuring security at every step in the data life cycle, from collection to destruction. PbD imposes a default position in favor of privacy, meaning that the data subject does not have to take action to protect privacy. IT systems particularly need to embrace these concepts.[101] PbD has been embraced by the TSA in its operational planning.[102] The approach is also endorsed in the NIST Privacy Framework.

An example of PbD is a system where the airport has limited access or control over a biometric, such as a system where the biometric is encoded and stored directly in access media issued to the individual (smart card) or on an individual's device (cellphone).

6.5.1 Privacy Impact Assessment

The development of a PIA for the capture and use of biometrics can help airports assess privacy considerations across the full cycle biometric data management, from collection to destruction. DHS has embraced this approach across all programs, including CBP's TVS program[103] and TSA's CAT program.[104] These PIAs offer formatting examples for airports. Another example of a PIA is found in the GAO report evaluating the TSA and CBP programs.

The PIAs use the FIPPs framework as a guide for analysis. The FIPPs principles should serve as a touchstone for both the development of policies around biometric data and other PII, as well as for evaluating compliance with those policies. Airports should assess their current privacy policies to ensure FIPPs are addressed. While FIPPs requirements are not legally mandated, they are generally accepted as a solid foundation for privacy management. See Section 6.2.3 for more details on FIPPs.

6.5.2 Retention

Retention is an important part of privacy management. It can also be a complex challenge for airports. Depending on the jurisdiction, the period of retention may be subject to state and local records retention requirements. Many states and localities have statutes or ordinances that direct the retention period for information collected by governmental entities. ACRP LRD 42 contains a detailed discussion of retention issues for data.

Where data retention is not controlled by external requirements, the airport should ensure that retention is consistent with the purpose of data collection and that the retention period is aligned with data minimization.

[100] Ann Cavoukian, Privacy by Design, Information & Privacy Commissioner (Jan. 2011), Cited at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[101] National Academies of Sciences, Engineering, and Medicine. *Legal Implications of Data Collection at Airports*. Washington, DC: The National Academies Press, 2021. Cited at https://doi.org/10.17226/26207.

[102] *TSA Biometrics Strategy*, prepared by Transportation Security Administration (July 2018). Cited at https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[103] Customs and Border Protection, "Travel Verification System" Privacy Impact Assessment DHS/CBP/PIA-56. Cited at (November 14, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[104] Transportation Security Administration, "Travel Document Checker Automation-Digital Identity Technology Pilots" Privacy Impact Assessment, DHS/TSA/PIA 51 (January 14, 2022). Cited at https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-tsa051-digitalidentitytechnologypilots-january2022_0.pdf.

Data retention also needs to align with the capability of digital systems to store and maintain the data. Shorter retention periods may reduce storage and related costs, such as the cost of responding to open records requests (although most open records law provide an exception for the production of PII like biometrics). Airports need to also understand and comply with state and federally mandated requirements surrounding the destruction of materials when they are no longer required for retention. Where possible, the data should be destroyed when the purpose for retaining the data ends. In the case of biometric information collected for access control, that would suggest eliminating the data when access is no longer permitted. Airport legal counsel should be consulted to identify jurisdiction-specific requirements. In the absence of specific requirements, airports may consider consulting the FTC's guidelines for consumer data.

Airports should work with their counsel to ensure that a written records retention policy is established. The airport also needs to ensure that auditing and internal controls are established to ensure that the retention schedule is followed.

6.5.3 Cybersecurity

Cybersecurity is a significant concern across the aviation enterprise. TSA has focused attention on airport efforts to identify and mitigate cyber threats. PII, including biometric data, is frequently the target of cyberattacks. Safeguarding information from cyber penetration is important from both security and liability perspectives.

Airports need to ensure that the measures employed to safeguard data are proportionate to the sensitivity of the data collected. In the case of PII, the standards for data protection should be high and should include measures like encryption and strict controls over data access. Airports need to work with their attorneys and IT professionals to ensure that their measures are commensurate with risk.

In March 2023, TSA issued Joint Emergency Amendment TSA-EA-23-01, which requires certain TSA-regulated airport and aircraft operators to develop an implementation plan to improve their cybersecurity and assess the effectiveness of those measures. A TSA press release summarized the measures as follows:[105]

- Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa;
- Create access control measures to secure and prevent unauthorized access to critical cyber systems;
- Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations; and
- Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.

[105] TSA-EA-23-01is only available to authorized users on the Homeland Security Information Network, but is summarized in a TSA press release: https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

SECTION 7: BIOMETRIC DEPLOYMENT CONSIDERATIONS

Most items in the checklist below cover biometric use in both access control and the passenger journey. Specific items for access control or passenger journey are indicated as such.

PLANNING AND IMPLEMENTATION

- Security Enhancement: The value that biometric verification adds in addressing any known threats
- Operational Efficiency: Impact of adding biometrics (throughput, additional process requirements for enrollment and infrastructure)
- User Acceptance: Perceptions, preferences, and willingness of users to adopt and follow guidelines for the new technology
- Regulatory and Compliance: Ensuring deployments meet any regulatory requirements
- Reputational Issues: Perception that the airport is taking reasonable measures while addressing security concerns and maintaining efficient operations
- Stakeholder Engagement: key stakeholders, including security, legal, facilities, and end users should be informed and included in key decisions and impacts throughout the entire life cycle of the project

NEEDS ASSESSMENT

- Perform baseline study of existing processes
- Enlist stakeholder involvement
- Perform a Needs Assessment covering any gaps, enhancements, or other opportunities in which biometrics can improve the security posture of the airport or enhance the passenger journey. Consider environmental factors, security needs of the access points, and user population (including any ADA requirements)
- Prioritize areas of vulnerability and build a deployment strategy around that prioritization
- Determine which biometric(s) best meet the project needs as determined by the Needs Assessment

LEGAL & SECURITY

- Research state and local laws and codes regarding the collection, use, and retention of biometric data
- Develop protocols for obtaining user consent and providing transparency regarding data use where appropriate
- Engage airport information security stakeholders to ensure policies are created and followed for biometric data handling; stakeholder examples include the Chief Information Security Officer, Chief Security Officer, IT Security, and Legal
- Develop robust protocols for secure storage and protection of biometric data (encryption, access controls, and monitoring mechanisms) and limit access and use of biometric data to defined security-related purposes consistent with policies and practices
- Use FIPPs analysis and consider conducting a PIA in assessing biometric collection and use practices

- Develop policies and procedures for people who cannot be enrolled in a particular biometric

TECHNOLOGY ASSESSMENT

- Assess the hardware and software operating the current identity verification process
- Assess the hardware and software used in conjunction with ID media issuance (for access control deployments)
- Consider putting out an Request for Information with general requirements to review available technologies that meet airport needs. Review reliability and performance, user experience, system scalability, and company stability, innovation, and track record of successful deployments
- Set up a test lab where various biometric devices can be tested with existing system(s) for compatibility and functionality
- Evaluate different biometric modalities (e.g., fingerprint, iris, face) based on accuracy, reliability, and suitability for the airport's needs
- Evaluate the biometric system's resistance to spoofing, tampering, or unauthorized access
- Conduct a pilot for field testing and evaluation of the technology before full-scale deployment
- Adjust full-scale deployment plans based on pilot results
- If storing biometric data on a smart card, ensure the selected media can store the biometric template and any additional data

REQUIREMENTS DEVELOPMENT

- Consider functionality, interoperability, regulatory, and security requirements
- Specify performance metrics such as matching speed, FAR, and FRR
- Consider all infrastructure needs, including networking, power, and cabling
- Consider all hardware requirements: workstations, servers, enrollment devices, badge media, biometric readers, etc.
- Consider all possible integrations required for the biometric system, including existing systems, third-party systems, etc.

TRAINING

- Develop training programs for system administrators, operators, and end users – emphasize the importance of data protection, privacy, and compliance
- Ensure enrollment staff are trained to enroll the highest quality biometric and perform test verifications after enrollment
- Ensure enrollment staff understand the data being gathered, how it is stored, and how it is used so they can answer enrollee questions
- Ensure enrollment staff understand the policies and procedures for people who cannot be enrolled into a particular biometric
- For access control, ensure that employees receive instructions on use at time of enrollment and test their credential prior to leaving the enrollment site

CHANGE MANAGEMENT

- Identify and be prepared to address possible resistance or concerns from users
- Create a Communications Plan for delivering changes to the user population

- Provide training opportunities and/or onsite guidance on biometric use (e.g., feet placement stickers for proper body position at a facial recognition reader or how-to videos as part of employee onboarding)
- Assess the hardware and software used for identity management systems (for access control deployments)

MAINTENANCE

- Include maintenance and support in budgetary estimates
- Understand the maintenance requirements for the evaluated technologies
- Establish regular maintenance schedules for hardware, applications, and device updates
- Monitor system performance and conduct periodic audits to ensure functionality and compliance
- Maintain clear documentation, including user manuals, troubleshooting guides, and system configurations
- Develop contingency plans for situations like system failures, power outages, or maintenance activities. Consider backup procedures, alternative access control measures, and communication protocols to minimize disruption and ensure continuous operation
- Engage in discussions and consider contract arrangements with software and hardware partners to help ensure the availability of replacement parts, support, and service for all components of the biometric solution during the system's expected useful life

REFERENCES

ADOT Motor Vehicle Division. Mobile ID. (n.d.). https://azdot.gov/mvd/services/driver-services/mobile-id.

Allen, Carolyn. "Verification (1:1) and Identification (1:N) Explanatory Graphics." Biometrics Institute, February 16, 2024. https://www.biometricsinstitute.org/verification-11-and-identification-1n-explanatory-graphics/.

Biometric Information Privacy Act, 740 ILCS 14/1. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Boston Ordinance No. 16-62. Civil Code Division 3, Part 4, Title 1.81.5. https://www.universalhub.com/files/recognitionban.pdf.

Buolamwini, J. & Gebru, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research*. Vol. 81, 2018, pp1-15. Conference on Fairness, Accountability & Transparency. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

California Consumer Privacy Act of 2018, Civil Code Division 3, Part 4, Title 1.81.5. https://transcend.io/laws/cpra/#section-1.

California Privacy Rights Act (2020). https://transcend.io/laws/cpra/#section-1.

Carpenter v. U.S. ___ U.S. ____, 569 U.S. 435, 138 S.Ct. 2206 (2018)

City of Portland Ordinance, Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City. (September 9, 2020). https://static1.squarespace.com/static/5967c18bff7c50a0244ff42c/t/5f3ad787ba3fd27776e444af/1597691785249/Ordinance+to+ban+use+of+FRT+in+Places+of+Public+Accommodation+plus+code+amendment+-Final.pdf.

Colorado Privacy Act, Colorado Revised Statutes, Part 13, Sec. 6-1-1301 (eff. July 1, 2023). https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.

Cornell Law School, Legal Information Institute. *"Unfair methods of competition unlawful; prevention by Commission."* (n.d.). https://www.law.cornell.edu/uscode/text/15/45.

Cothron v. White Castle Systems, Inc., 2023 IL 128004 (Feb. 17, 2023)

Delta Airlines. "Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers." *Delta News Hub*, 2020. https://news.delta.com/deltas-exclusive-partnership-tsa-streamlines-check-security-atlanta.

Delta Airlines. "Delta Opens First Biometric Self-Service Bag Drop in U.S*."* *Delta News Hub*, 2020. https://news.delta.com/deltas-exclusive-partnership-tsa-streamlines-check-security-atlanta.

Facebook Biometric Information Privacy Litigation, 522 F. Supp. 3d 617 (N.D. Cal. 2021)

Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Congress (2021). https://www.congress.gov/bill/117th-congress/senate-bill/2052.

Federal Aviation Administration. *Access to Airports by Individuals with Disabilities Advisory Circular, No: 150/5360-14A*. December 6, 2017. https://www.faa.gov/documentLibrary/media/Advisory_Circular/150-5360-14A.pdf.

Federal Bureau of Investigation. *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling*. FedID, Version 1.0, Dec. 2020. https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments/firs-iafis.

Federal Bureau of Investigation. *Next Generation Identification (NGI).* (n.d.) https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi#:~:text=The%20Next%20Generation%20Identification%20(NGI)%20Iris%20Service%2C%20provides%20a,repository%20within%20the%20NGI%20system.

Federal Trade Commission. *Disposing of Consumer Report Information? Rule Tells How*. September 13, 2021 https://www.ftc.gov/business-guidance/resources/disposing-consumer-report-information-rule-tells-how.

Federal Trade Commission. *Privacy Online: A Report to Congress*. June 1998. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

Find CLEAR Near You. (n.d.). https://www.clearme.com/where-to-use-clear.

Garg, Suneet., "A Critical Study and Comparative Analysis of Multibiometric Systems using Iris and Fingerprints." *International Journal of Computer Science and Information Security*. https://www.academia.edu/12236182/A_Comparative_Study_of_some_Biometric_Security_Technologies.

General Accountability Office 2020. "*Facial Recognition CBP and TSA are Taking Steps to Implement Programs, but CBP should Address Privacy and System Performance Issue*" GAO 20-568. https://www.gao.gov/assets/gao-20-275.pdf.

General Accountability Office 2020. "*TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*" GAO 20-275. https://www.gao.gov/assets/gao-20-275.pdf.

General Accountability Office 2020. "*Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*" GAO 20-522. https://www.gao.gov/assets/gao-20-522.pdf.

German R., Barber S.K., *Consumer Attitudes About Biometric Authentication. The University of Texas at Austin*, May 2018. https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf.

Grassi, P., Garcia, M., & Fenton J., *Digital Identity Guidelines*, National Institute for Standards and Technology NIST Special Publication 800-63-3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Grother, P., Ngan, M., & Hanaoka K., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* National Institute for Standards and Technology https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

Illinois Biometric Information Privacy Act, 740 ILCS 14/15.

Illinois Biometric Information Privacy Act, 740 ILCS 14/20

International Airport Review "Successful Biometric E-Gate at LAX Blazes Trail for Commercial Aviation." *IAR News*, January 2018. https://www.internationalairportreview.com/news/64154/biometric-e-gate-lax-aviation.

International Standards Organization "Personal Identification ISO Complaint Driving License Part 5 Mobile Driving License (mDL) Application." *ISO,* September 2021. https://www.iso.org/standard/69084.html.

Katsanis, Sara H., et. al., "U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics," *IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY*, VOL. 3, NO. 1, (March 2022). Cited at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9576819

King v. Maryland, 569 U.S. 435 (2013).

Maryland Department of Transportation. *“Maryland Mobile ID in Apple Wallet.”* (n.d.) https://mva.maryland.gov/Pages/MDMobileID_Apple.aspx.

Mason, Marcy. “Biometric Breakthrough*” Frontline Magazine*, September 28, 2022. https://www.cbp.gov/frontline/cbp-biometric-testing.

Merkley, Hon. J., et al., “*Letter to Administrator David Pekoske.”* The United States Senate, February 9, 2023. https://subscriber.politicopro.com/f/?id=00000186-3c87-d37d-a7e7-3fefde670000.

Motion 2019-13, *A Motion of the Port of Seattle Commission.* Port of Seattle Com’n Meeting Dec. 10, 2019. https://www.portseattle.org/sites/default/files/2019-12/Motion%202019-13__Biometrics%20Principles.pdf.

National Conference of State Legislatures. “*Data Disposal Laws.”* January 4, 2019. https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

National Conference of State Legislatures. “*Data Security Laws: Private Sector.”* May 29, 2019. https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws.

National Conference of State Legislatures. “*Data Security Laws: State Government.”* February 14, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx.

National Conference of State Legislatures. “*Security Breach Notification Laws.”* July 17, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Oakland Municipal Code 9.64. https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE_9.64.045PRACUSBISUTEPRPOTE#:~:text=A%20summary%20of%20community%20complaints,subject%20to%20the%20technology's%20use.

Practical Law Data Privacy Advisor. “Baltimore Enacts Facial Recognition Moratorium.” *Thomson Reuters Practical Law,* September 7, 2021. https://news.delta.com/deltas-exclusive-partnership-tsa-streamlines-check-security-atlanta.

Radio Technical Commission for Aeronautics, *DO-230L Standards for Airport Security Access Control Systems,* December 15, 2022. https://my.rtca.org/productdetails?id=a1BDm000000GuyNMAS.

Rotenberg, Marc, et al. “Letter to The Honorable Bennie Thompson, Chairman The Honorable Mike Rogers, Ranking Member Committee on Homeland Security U.S. House of Representatives.” *Epic.org*, February 5, 2020. https://www.biometricupdate.com/202208/cat2-request-goes-out-for-facial-recognition-at-us-airports.

San Francisco Administrative Code Ch. 19B. https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

Texas Business and Commerce Code Ch. 503. (n.d.) https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

Telos Corporation. “Telos Comparison of Mobile Biometric Modalities.” *Telos*, https://www.ojp.gov/pdffiles1/nij/nlectc/211839.pdf.

TSA. "*Identity Management*.” Paper presented at the ACI-NA PS&S/ACC Security Technology Conference, Arlington, VA, October 19, 2022.

TSA. “Biometric and Digital Identity Solutions for TSA PreCheck Members.” (n.d.). https://www.tsa.gov/digital-id.

TSA. "*TSA Biometric Roadmap, For Aviation Security & the Passenger Experience*" 2018. https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

TSA. "*TSA Insider Threat Roadmap.*" 2020. https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

TSA. "*TSA Identity Management Roadmap for Transportation Security and the Credential Population and Passenger Experience*." Feb. 2022. https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf.

TSA. "*TSA issues new cybersecurity requirements for airport and aircraft operators.*" National Press Release. March 7, 2023. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft.

TSA. "*TSA Travel Document Checker Automation-Digital Identity Technology Pilots.*" January 14, 2022. https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-tsa051-digitalidentitytechnologypilots-january2022_0.pdf.

United States Government Accountability Office. "*Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and Performance Issues*." *GAO,* 20-568, Sept. 2020. https://www.gao.gov/products/gao-20-568.

U.S. Customs and Border Protection (CBP). *Biometric Air Exit Business Requirements* Version 2.0. January 2020. https://archive.epic.org/foia/dhs/cbp/biometric-entry-exit/Face-Recognition-Air-Entry-Final-Report.pdf.

U.S. Customs and Border Protection (CBP). *Privacy Impact Assessment for the Travel Verification Service* DHS/CBP/PIA-056. November 18, 2018. https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf .

U.S. Customs and Border Protection (CBP). *"Privacy Information – Biometric Boarding"* (2019). https://www.cbp.gov/sites/default/files/assets/documents/2020-Feb/3.%20Biometric%20AIR%20EXIT%20SIGNAGE%20-%20FINAL.pdf.

U.S. Customs and Border Protection (CBP). *"Say hello to the new face of efficiency, security and safety"* (n.d.) https://www.cbp.gov/travel/biometrics.

U.S. Department of Commerce, National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. Version 1.0. January 16, 2020. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

U.S. Customs and Border Protection(CBP). "Preclearance" (u.d). https://www.cbp.gov/travel/preclearance.

U.S. Customs and Border Protection (CBP). *Travel Verification System* DHS/CBP/PIA-56. November 14, 2018. https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

U.S. Department of Homeland Security (DHS). "*Privacy Impact Assessment for the Travel Document Checker Automation—Digital Identity Technology Pilots*." DHS/TSA/PIA-051, Jan. 14, 2022. https://www.dhs.gov/publication/dhstsapia-051-travel-document-checker-automation-digital-identity-technology-pilots.

U.S. Department of Homeland Security (DHS). "*Privacy Policy Guidance Memorandum*." DHS Privacy Office Memorandum Number 2008-01, December 28, 2008. https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

U.S. Department of Homeland Security (DHS). "*Privacy Policy Guidance Memorandum*" DHS Privacy Office Memorandum Number 2017-01, April 25, 2017. https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

U.S. Department of Homeland Security (DHS). "*US-Visit, Biometrics and You Form DHS-M-1-English.*" U.S. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_brochure_english.pdf.

Utah Consumer Privacy Act of 2018. Utah Code Annotated, 13-61-101.

Utah Department of Public Safety. (n.d.) https://dld.utah.gov/utahmdl.

Virginia Consumer Data Protections Act. Code of Virginia, Chapter 53, Section 59.1-575 et. seq. (Effective January 1, 2023) § 59.1-575. (Effective January 1, 2023) "Definitions." *Virginia.gov*.

Washington Revenue Code Ch. *19.375.* (n.d.) https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true#:~:text=(1)%20A%20person%20may%20not,identifier%20for%20a%20commercial%20purpose.

Waterson, Leonardo Sam, "Best Biometric Modality Based on their Strengths and Weaknesses." *M2SYS,* 2019. https://www.m2sys.com/blog/biometric-technology/best-biometric-modality.

APPENDIX A: ACCESS CONTROL CASE STUDIES

Examining the biometric access control applications currently in use at airports offers important lessons on possible implementation models, including examples of the complexity of the integrations and their impacts on credential issuance.

A1: Fingerprint Biometric for Access Control – This case study reviews two large airports that have had fingerprint biometric programs for over ten years and utilize similar biometric reader and access control technologies.

A2: Dual-Use Facial & Fingerprint Biometric for Access Control – This case study reviews a large airport that operates two biometric modalities in their access control system. The airport introduced fingerprint biometric access control in 2006 and added a facial biometric system in 2018.

A3: Facial Biometric Pilot for Vehicle Access – This case study discusses a biometric vehicle access control program intended to process vehicles at speed at midfield access checkpoints to reduce current queuing issues.

A4: Facial Biometric Pilot for Access Control – This case study describes the airport's pilot program to add facial biometric for access control. The airport previously used hand geometry biometric devices but discontinued their used during the COVID-19 pandemic.

A5: Fingerprint Biometric for Access Control (Two Airport System) – This case study describes two airports that were among the first in the US to deploy biometrics in an operational setting. Both airports use separate instances of the same biometric/access control/credentialing system.

A6: Iris/Fingerprint Biometric for Access Control (Canada) – This case study describes the centralized biometric access control program deployed at Canadian airports. While the centralized nature of the system has no current applicability to US airports, the lessons of its use of both fingerprint and iris biometrics can be helpful to airports considering those technologies.

A.1. Fingerprint Biometric for Access Control

OVERVIEW

This case study reviews two large airports. They have both had fingerprint biometric programs for over ten years and utilize similar biometric reader and access control technology. They also have access control programs that are integrated with other security technologies like CCTV.

Airport A
Airport A is a state-owned CAT X airport operated under the state's Department of Transportation. Within that Department, the State Aviation Administration serves as the airport's governing body. The airport has approximately 500 regulated doors and about 12,000 badged aviation workers.

Within the Division of Operations and Maintenance, the Office of Airport Security is responsible for maintaining the Integrated Airport Security System (IASS) in partnership with the Division of Airport Technology. The airport badging, video management, and access control systems (including biometric readers) are all segmented within the IASS. While the IASS is the responsibility of the Office of Airport Security, the airport has utilized a contractor to maintain the system since the originally was installed, circa 2011. This airport uses an IDMS in their badging process.

Airport B
Airport B is a CAT X airport that is operated jointly by a city/county government. The airport has approximately 500 regulated portals and 23,000 badged aviation workers.

The Airport Safety and Security Department is responsible for the overall operation of the technology supporting airport security operations. The airport has an integrated security system that includes access control and a video management system. The systems are maintained by the contract integrator. This airport also uses an IDMS in their badging process, but it is from a different vendor than Airport A.

SYSTEM DESCRIPTION

Both airports have deployed Innometriks Rhino biometric fingerprint readers, which conduct a 1:1 comparison with the fingerprint template encrypted on the badge, but are also capable of using a PIN in conjunction with the airport badge. The biometric evaluation is conducted at the edge by the individual reader from data stored within the reader itself. That data is routinely refreshed by the centralized badging database.

Neither airport accommodates 1:N comparisons at biometric readers, owing to infrastructure limitations on connectivity of readers with the central database.

Reader placement at portals includes considerations for ADA compliance. At the time of purchase, the cost per reader was approximately $3,500.

DEPLOYMENT STRATEGY

Airport A
Airport A has deployed the Rhino readers at critical locations within the airport, such as the Federal Inspection Station within the Customs and Border Protection Area, administration offices, and public-to-Sterile Area access points.

Prior to activating the biometric capability at its portals, the airport conducted a pilot test at a highly used access portal to assess functionality and user acceptance. The testing revealed some user resistance because the Rhino system's keypad was different than the previous badge reader (HID RK40 iClass SE), and its programming required a longer transition time between individual transactions. Both factors contributed to a slight decrease in throughput. Once the programming issue was resolved, users adjusted to the modification and the airport deployed the new readers at the previously identified locations.

Airport B

Airport B followed a slightly different deployment strategy and path for technology rollout than Airport A. In this case, the fingerprint biometric was selected to replace hand geometry readers as part of a terminal renovation plan.

The process of replacing the hand geometry readers with fingerprint readers was lengthy. The project commenced in 2011 and was not completed until 2018. Biometric readers were deployed at both indoor and outdoor locations, including all regulated doors in the airport (approximately 500) and access-controlled vehicle gates. In some cases, covers were created for the outdoor readers to help cut down on glare and protect them from the elements.

Airport B noted general acceptance of the biometric fingerprint technology by aviation workers. Once trained in conjunction with the enrollment process, personnel were able to use the deployed readers to gain access. Individuals whose prints were determined to be unreadable at enrollment are allowed access through use of a proximity (prox) card and PIN.

The airport did not observe appreciable throughput issues. In some high traffic areas, throughput concerns were addressed with the addition of multiple access points.

Airport B reported no significant maintenance or performance challenges with the readers, and characterized as them as “dependable.” Maintenance of the readers is conducted by the airport’s technical service group. The airport is experiencing some supply change challenges with respect to the current readers.

OPERATIONAL SECURITY FOCUS

Airport A

Airport A’s operational security focus was to enhance security in critical locations. The biometric readers in these locations require two-factor authentication, consisting of an airport badge swipe and biometric fingerprint. The ability exists to raise and lower the security level for each portal within the access control system, with badge swipe plus PIN being the lowest and badge swipe plus biometric fingerprint being the highest security level. In addition, each access portal has its own assigned clearance; the biometric encoding of a badge does not necessarily afford access to all biometrically secured portals. Access permissions need to be granted within the IDMS where access is managed to every secured portal within the IASS ecosphere.

Airport B

Airport B’s operational security focus was broader than that of Airport A, evidenced by the higher number of portals secured with biometric access control. Like Airport A however, Airport B maintained different authentication requirements at some portals or access points based on security concerns. For example, Airport A has deployed prox readers for aviation employees using checkpoints but there is no use of biometric readers at those access points. Airport B does not use mobile biometric readers.

PROCUREMENT

Airport A

Airport A’s selection of technology was part of a larger procurement to upgrade an entire suite of systems to support security operations. The original RFP was developed in 2010 for both construction and maintenance contract requirements. The work included major subsystems within the IASS, including the Digital Video Management System, Storage Area Network, Identity Management System, and all airport badge readers. This multi-million-dollar project also included new cameras and all the electrical work throughout the airport that was specifically related to the IASS.

A two-year allocation was given to complete the construction, followed by a five-year maintenance agreement to ensure the entire IASS was maintained to meet the requirements of the contract. At the conclusion of the original maintenance contract, new contracts were awarded to maintain, replace, and expand the original system.

Airport B

Airport B reported that their system was also selected through a competitive procurement process that was part of a larger package of improvements in connection with a terminal upgrade project. That project included a rip and replace of the existing hand geometry biometric technology. The project took seven years to complete.

ENROLLMENT

Airport A

Airport A captures biometric and biographical information during the enrollment process in their IDMS. Individuals who require access to the biometric readers must have their airport badge encoded with the fingerprint capture. For individuals whose prints are unreadable, that fact is notated and they are allowed to use a PIN as their second authentication factor.

Prior to generating the airport badge, the Trusted Agent ensures the index finger is captured on the right and left hand. Capturing both left and right fingers provides the applicant with an alternative if one does not read correctly on the access control reader. After the badge has been printed, the Trusted Agent will encode the airport badge with the fingerprints. Since the fingerprints have been captured within the IDMS the need to capture new fingerprints is not required during the airport badge renewal process unless there has been a change to one of the enrolled fingers.

To ensure that a new badge is properly encoded, whether the badge is a renewal or initial issue, it needs to be tested. After creating the badge Trusted Agents require applicants to test all newly printed airport badges to ensure they work as required prior to leaving the badging office.

First Responders, Federal Partners and State employees are the primary individuals who have airport badges encoded with biometric access privileges. Even though the airport badge has been encoded, it does not mean the applicant has access to every reader. Access is assigned to each individual for required portal access.

Security of PII data maintained in both the IDMS system and in the access control system is a matter of concern. Both systems have encryption and other data security protocols to secure the stored data.

Airport B

Airport B follows an enrollment process like that of Airport A. A fingerprint biometric is taken at enrollment and is encoded on the badge. Badges are tested by the badge holder before leaving the badging office to ensure the badges are functional. This also has the benefit of orienting the badge holder to the access control system and proper use of the badge. As with Airport A, individuals with unreadable prints are allowed to use a PIN code as a second factor for authentication at portals equipped with biometric readers. Airport B noted no difficulty or significant additional time occasioned by the collection and encoding of the fingerprint biometrics in connection with badging. Airport B’s IDMS also stores the biometric fingerprint template that is stored on the card.

FUTURE PLANS

Airports A

Airport A is currently examining measures to replace all existing "end of life" airport prox card badge readers. Studies are underway to review new biometric access technologies to replace the existing fingerprint biometric readers.

Airport B

Airport B is also examining options for replacement of its current fingerprint biometric system. Supply chain and procurement challenges with the current product vendor have prompted this effort. The movement to new technologies is constrained by the current infrastructure supporting the existing system. The existing card technology and IDMS cannot support movement to a facial biometric. The airport is also confronted with a local political environment and restrictive ordinance that limit facial biometric applications. Physical infrastructure like power and cabling also restrict the ability of real-time connection with the central database from all access points. This means that, absent significant and costly infrastructure changes, the selections of solutions are limited to those that provide a 1:1 comparison with biometric information encoded on badges.

A.2. Facial & Fingerprint Biometric for Access Control

OVERVIEW

This large, Western State airport operates as a department of the city government. It is self-supporting, using no local or state tax dollars for operations or capital improvements. The airport has a badged population of over 38,000 aviation workers, and 15,000 of those workers are airline employees. Despite its large geographic footprint, it maintains a common automated access control system (ACS) across all routine access gates and tenant facilities. The ACS currently processes over six million transactions per month. There are over 150 doors controlled by biometric access control using facial and/or fingerprint modality.

The airport has multiple business units. The Security unit, which reports up through the Operations department, is responsible for the access control and biometric program. The Security unit has IT personnel and one IT project manager who are direct airport employees. Technologies supporting the security program run on a dedicated network. The airport's IT department manages cybersecurity in conjunction with the Security department. The airport's organizational structure with dedicated IT assets facilitates the development of technology solutions to support security operations.

The airport also uses the services of a local integrator to assist in the operation of their ACS and biometric technology. The integrator developed a custom fingerprint biometric program and managed the integration of facial biometric technology with the airport's ACS.

The airport has not changed its underlying ACS since it was constructed in the 1990s. The biometric features were a later addition developed by the integrator that built the ACS. The facial biometric was purchased from a separate vendor, but the ACS integrator developed an interface to align it with the existing ACS.

SYSTEM DESCRIPTIONS

Fingerprint Recognition System

Around 2006, the airport introduced fingerprint biometric access control. Currently the airport has over 100 fingerprint biometric readers deployed at 40 access areas (both indoor and outdoor).

The airport is now operating their second generation of fingerprint readers. The first generation had the fingerprint placement on a gold foil background, which presented maintenance challenges as users would damage the reader heads, both intentionally and unintentionally (heavy use). Those readers were replaced by finger-swipe readers designed by the ACS integrator. The airport is currently experiencing parts challenges with this system due to the proprietary design.

The fingerprint biometric system is capable of 1:1 comparison of fingerprints to templates maintained in the ACS database. That comparison is triggered by the presentation of the badge, which refers to a database record containing the fingerprint template associated with that badge. The system also verifies that the presented credential is active before reading the fingerprint. The badges are not smart cards, and no biometric data is stored on the card.

Facial Recognition System

The airport deployed a small number of infrared facial biometric readers in 2018, and has gradually expanded to approximately forty facial systems across more limited access areas than the fingerprint readers. This was one of the first facial biometric deployments in airport access control. The readers are used at approximately twenty-five interior portals in five different areas of the airport. The portals are also equipped with fingerprint biometric readers.

The ACS integrator created a custom interface to incorporate the new facial biometric readers with the ACS. Like the fingerprint readers, the facial readers operate on a 1:1 comparison of the face to a template maintained in central database. When the individual seeking access presents their badge to the prox reader, the central database references the template related to that particular badge. The system also verifies that the presented credential is active. As with the fingerprint biometric, no facial biometric data is stored on the card. All facial biometric readers are located indoors; the readers are not rated to operate outdoors.

The manufacturer has stopped production of the facial biometric readers and discontinued support. The airport has stockpiled the previously manufactured readers to support itself while it develops a transition plan. The airport is currently conducting a pilot of a new facial recognition system at a facility linked to the airport's ACS. If procured, this new technology will require enrolling all users with a new facial template.

SELECTION AND PROCUREMENT

The selection team for the biometric systems consisted of airport stakeholders from both the IT and Security departments. The IT section of the airport has a dedicated IT project manager to assist in the process of IT support system development and deployment.

The biometric systems were procured under an existing contract for the airport's ACS. The facial biometric reader purchased and utilized to date cost approximately $3,800 per unit, exclusive of installation cost. The new facial readers the airport is considering are $4,200 per unit.

The cost of the fingerprint biometric units is more difficult to quantify because they are covered under the general ACS agreement. The systems integrator for the ACS designed and manufactures the fingerprint biometric readers that are part of the ACS system.

In addition to the cost for the fingerprint and facial biometric reader units, there are costs associated with the software that maintains the database and provides the template data for the biometric readers to match.

As part of planning for the initial facial biometric deployment, a pilot evaluation was conducted through Safe Skies' ASSIST program. That evaluation included testing the system both at the airport and at Safe Skies' facility.

DEPLOYMENT STRATEGY

The airport's deployment strategy was to place biometric devices on "First Entry Portals" into the airport's Sterile and Secured environments (i.e., public-to-Secured or public-to-Sterile portals), which were considered the highest risk security points. Most of these portals were public-to-Secured access points. This strategy achieves the goals of enhanced security without additional expense.

Some aviation workers who only have access to Sterile Areas enter through the passenger screening checkpoints. The Sterile-to-Secured Area access points use proximity badge read and PIN, but since all persons entering the Sterile Area have been through either a biometric authentication process or some form of screening or inspection, no additional biometric screening is deployed at these access points.

The initial rollout of fingerprint biometrics occurred over a number of years, with deployments expanding to cover all First Entry Portals in accordance with the airport deployment strategy.

Badge holders with unreadable fingerprints enter via 24-hour employee turnstiles where they use prox and PIN readers. They are subject to additional physical inspection by staff posted at those entry points. The airport reported that a couple hundred aviation workers have unreadable prints.

The pilot program for the facial biometric began in February 2018. After the pilot completion, the airport slowly added readers to access control locations that were covered by existing fingerprint readers, but the fingerprint readers remained in place affording users the ability to select their preferred method of biometric verification. Since not all badged employees were enrolled in the facial biometric, that method of verification was not always available to individuals, even if both reader types were present. (See Enrollment and Training below.)

No biometric readers are used at vehicle access gates to Secured Areas. Instead, prox and PIN are used, and gates are staffed with personnel responsible for confirming the identity of vehicle occupants.

ENROLLMENT AND TRAINING

The initial training on the systems and enrollment processes were provided by the systems' respective vendors. Those responsibilities were transferred to the airport's business technology unit.

The badging office staff is responsible for orienting aviation workers to the different biometric systems in use at the airport. This occurs in connection with the enrollment process at the time of badge issuance. Aviation workers, once provided with badges, are required to test the badges at "test readers" before they leave the badging office.

The airport has a four category badging system (colors anonymized):

- White for public area access only
- Green for Sterile Area access only
- Red for Sterile and Secured Area access
- Purple for Sterile and Secured Area access with escort privileges

All Green, Red, and Purple badge holders are enrolled into both biometric access systems. The process for enrollment requires the collection of biometric information with fingerprints and facial images stored as encrypted templates in the centralized databases that are integrated with ACS. This means every cardholder in those categories is required to undergo two biometric enrollment processes for the creation of separate face and fingerprint templates.

The badge renewal process does not require any additional capture of biometric information. Because the biometrics are stored in a database and generally do not change, no re-enrollment is required, except in the rare circumstance where there is a biometric change (e.g., scarring on or loss of a finger, or some facial disfigurement). If a new biometric template is required for the use of a new biometric system, then that biometric may be enrolled during the badge renewal.

The airport has an IDMS, but that system does not store biometric templates. The templates are maintained solely in the ACS.

EFFICIENCY AND EFFECTIVENESS

The introduction of biometrics had an immediate impact on the airport through increased security and restricted employee access at biometric deployment sites. Both systems were piloted before deployment, and the airport was satisfied that both systems provided adequate assurance that improper access would not be granted and operational efficiency was maintained.

The airport experienced the following challenges relative to the fingerprint biometric system:

- Approximately 200 aviation workers out of 38,000 have unreadable fingerprints
- The system has reduced performance in inclement weather
- A protective covering is required for outdoor surfaces

The airport experienced the following challenges relative to facial biometric system:

- The readers are not outdoor rated
- The readers have to be shielded from direct sunlight
- The readers are less effective if subjects are wearing glasses, sun protection factor (SPF)-rated facial makeup, brightly colored safety vests

The airport noted no significant challenges for gaining user acceptance of either biometric system. While the staff noted that some individuals tend to prefer one biometric authentication method over another, those choices are idiosyncratic. There is no noted efficiency advantage of one biometric system over another.

IT noted that the newer facial biometric reader is faster than the existing facial biometric technology. The reader also has greater efficiencies in its ability to pick up facial biometrics at various angles as the individual approaches the reader. It was also noted that there are no unreadable facial biometrics in the airport population.

Anecdotally, the airport staff noted that there was some increased preference for the touchless facial biometric during the COVID-19 pandemic. However, a significant numbers of individuals still opted to use the fingerprint biometric when both readers were available.

SYSTEM RELIABILITY AND MAINTENANCE

The airport noted that the fingerprint reader, as a touch-based system, requires regular routine cleaning of its sensor head. Conversely, the touchless facial system does not require regular cleaning. However, unlike the facial system, the fingerprint system has outdoor-rated portable readers and was reported to be less sensitive to environmental conditions.

Over time, both systems have experienced maintenance issues. The initially deployed fingerprint reader heads were damaged due to user actions, which prompted the airport to change to finger-swipe readers. While the swipe readers require routine reader head replacements, the airport does not find that to be a threat to the system's reliability, as the system has a predictable life cycle and the system integrator is able to make replacements to keep the system operating. However, as the system ages, securing replacement parts is becoming a challenge.

The airport also noted increasing challenges with the facial recognition readers. Reader life cycle information was not available at purchase (owing to the newness of the technology). While the system had an initial two-year warranty and requires no preventive maintenance, the readers have begun to fail as they age. The reasons for the failures are not readily apparent. The airport believes that the volume of transactions over time may be contributing to the failure rate. Because the manufacturer has discontinued the readers, the airport has stockpiled readers to keep the system operational, but has concluded that the system will need to be replaced after only a five-year deployment.

FUTURE PLANS

The airport plans to continue the use of both fingerprint and facial biometrics with its ACS, since those biometrics complement each other and offer choices to aviation workers, but it is planning to upgrade or replace both existing systems due to development of new and better technologies, maintenance and replacement costs for the current systems, and the manufacturer’s decision to discontinue supporting critical equipment in the current systems. The airport is also considering a major overhaul of its entire ACS, but that will likely be a multi-year process of design and implementation.

The airport understands that the dual biometric strategy places additional burdens on the badging operation, including the need to enroll biometrics and create templates for each biometric solution. As the airport looks to transition to new biometric systems, cardholders will need to enroll separate templates for those systems. That means that until all the older readers are discontinued, each badge holder may need to complete up to four separate biometric enrollments.

The airport was briefly confronted with a potential legislative challenge to the use of biometrics for their access control, but no legislation prohibiting biometric use has yet been enacted.

A.3. Vehicle Access Pilot

AIRPORT OVERVIEW

This major metropolitan CAT X airport is one of the busiest in aircraft movements and passenger traffic. It has an expansive footprint that hosts critical infrastructure for aviation, passenger rail, water and wastewater treatment plants, energy infrastructure, information technology infrastructure and several government facilities, each subject to its own set of federal and state laws and regulations, and local ordinances.

The airport security organization falls under the Operations Division and works closely with the Finance and Information Technology Services Division.

PLANNED PILOT

The airport has initiated a biometric vehicle access control pilot to process vehicles at speed at midfield access checkpoints to reduce current queuing issues. The midfield checkpoint is the second access point from the SIDA to the Secured Area. Access control at the first access point consists of a badge swipe and security personnel review.

Currently the midfield checkpoint is staffed, and the vehicle driver swipes their badge, which is then viewed by security personnel staffing the checkpoint. The biometric system being piloted identifies the vehicle driver via facial recognition. The biometric reader is connected to the system's database, which verifies the identity of the individual and then communicates with the access control system to determine if that individual has the appropriate access.

The pilot is being conducted in two/three inbound lanes and one outbound lane. The driver's face image is captured as they drive at a designated speed in one lane. If the image is not successfully captured, the vehicle is directed to a second lane so as not to impede traffic. Once the image is successfully captured and identified, a barrier arm located further down the lane is raised to allow access. If all access fails, the vehicle is directed to a hold pad where they can contact the security access control office.

The system utilizes existing badge photos to enroll users. Signage has been installed as part of the pilot to guide badge holders on the process of using the system.

If the pilot is successful, the airport will deploy the system at three additional midfield checkpoints, as well as expand the biometric technology to other projects.

A.4. Facial Biometric for Access Control Pilot

OVERVIEW

This major metropolitan CAT X airport is one of the busiest in aircraft movements and passenger traffic. It has an expansive footprint that hosts critical infrastructure for aviation, passenger rail, water and wastewater treatment plants, energy infrastructure, information technology infrastructure and several government facilities, each subject to its own set of federal and state laws and regulations, and local ordinances.

The airport security organization falls under the Operations Division and works closely with the Finance and Information Technology Services Division.

The airport worked with Safe Skies to test various biometric devices and selected a facial recognition vendor as the system to pilot.

DEPLOYMENT STRATEGY

The strategy for deployment was to conduct a sixty-day pilot program on a single, medium-traffic door, review performance and, if successful, deploy the biometric technology to other employee portals. At the time the airport was interviewed, the program pilot phase was ending and construction was underway at employee portals.

SELECTION

The airport previously used hand geometry biometric devices at all access portals. During the COVID-19 pandemic, the airport shut off the hand geometry readers to reduce the potential spread of the disease, and reverted to the previous process of badge swipe and review by security personnel. This left the airport out of compliance with TSA regulations for two-factor authentication, but given the circumstances of the pandemic, staffing the portals was an acceptable measure given the timeframe to pursue and deploy an alternative biometric. The airport wanted to pursue a zero-touch biometric and chose facial recognition.

The review and selection team consisted of members of the airport Operations Division as well as members of the access control/security management groups.

ENROLLMENT AND TRAINING

Badge holders with access to the pilot door were enrolled in the facial recognition system prior to the pilot. This was done in conjunction with a pilot for multi-technology badge media as part of an access control upgrade so that a single badge would work with the existing and new access control systems. The users were given a scheduled time to visit the badging office to be enrolled. The badging office did not add any staff during this time, but allowed overtime to cover the additional enrollment schedule. During the first days of the pilot, trained personnel were stationed at the door to assist with device use.

For the overall access control program, new badge media has been issued and biometric enrollment was completed at the time of badge renewal.

EFFICIENCY AND EFFECTIVENESS

Overall, the facial recognition biometric technology has performed as expected, with the biggest challenges coming from badge holders learning to use the technology. This includes issues with hats and glasses, as well as learning to properly position themselves at the reader.

The airport placed an instructional placard at the reader and stationed personnel to assist users for the first few days of the pilot. Some users still struggled with positioning, so feet appliqués were placed on the ground to assist with proper body positioning.

Reports were run daily to review device performance. Initial results showed approximately 7–8% recognition issues. The vendor was contacted to review the system installation and configuration. The reader mount height was adjusted, and a configuration setting was added to allow for a second recognition attempt before denying the badge holder. The recognition issues dropped to 0.7%.

Further monitoring for timeouts and mismatches is being conducted, and individuals are being contacted by the badge office to review facial recognition reader use. In one instance, an older cardholder who is not technologically savvy placed his card badge photo up to the reader. With a few minutes of training, that user is now correctly using the device. The airport expects the recognition issues to drop to 0.5%.

FUTURE PLANS

Future plans are to place the facial readers at all employee portals. The first phase will be card and facial biometric with plans to move to only facial biometric at portals where dual-factor authentication is not required by TSA. This is for consideration of employees wearing their badge on an armband, where they have to turn to present the card, which may affect proper body positioning at the facial recognition reader. Note this is only if approved by the TSA.

A.5. Fingerprint Biometric for Access Control (Two Airport Comparison)

OVERVIEW

This airport system with two major airports is self-supporting, using no local or state tax dollars for operations or capital improvements. The airports generate more than $45 billion in annual economic activity and create 540,000 jobs for the region.

The airport organization, which manages all aspects of both airports, comprises seven business units: The Access Control and Biometric program falls under the Security Unit, with overlap into the Information Technology Unit where needed.

SYSTEM DESCRIPTION

Both airports use separate instances of the same biometric/access control/credentialing system. The system is upgraded as minor releases are issued, with major upgrades occurring approximately every four to five years to take advantage of new technologies, security enhancements, and added functionalities.

The fingerprint template is a hash that is stored in both a database and on the user's badge. At the reader, the finger is placed on the device and matched to the card-stored fingerprint template. Once verified, the user data is passed to the field panel or server to determine access rights.

DEPLOYMENT STRATEGY

These airports were among the first US airports to deploy biometrics in an operational setting. Beginning in approximately 2004, they began discussing and planning the use of biometric devices in high risk portals, where badge holders pass into Secured Areas. Pilot programs were used to test different device modalities and card technologies for functionality and compatibility with the existing access control system. This effort was implemented largely in response to increasing numbers of unaccounted for badges as well as reported misuse of badges.

The stakeholder engagement plan and continuing communications followed standard airport processes, allowing the biometric project manager to devise a systematic approach to ensure expectations, decisions, risk/issues, and project progress information is delivered to the right person at the right time with the most efficient and effective level of information.

Over time, the airport deployed more biometric readers in the field to manage access into Secured Areas. As the new biometric devices were deployed, especially in high traffic areas, the airport posted an officer to assist users with access issues (e.g., incorrect finger placement, failed reads).

Some people could not be enrolled in the fingerprint biometric system. The access control vendor had to quickly amend the application to allow for a PIN option for people who could not be enrolled. Some individuals could not be enrolled due to working with chemicals, thin skin present in some older individuals, and amputated appendages.

SELECTION AND PROCUREMENT

The selection team consisted of airport stakeholders from both the IT and Security business units with an existing managed service provider consultant group providing pilot installation, configuration, integration, and pilot program data. The team reviewed all available standards from NIST and Homeland Security, although 2004 was early for some of this work. Some considerations included:

- No storing of biometric images. Biometric data must be encrypted via an algorithmic process to ensure a low probability of assigning meaning to the data without use of a confidential process or key.
- The biometric initial design identified the badge holder matched the card and then required a PIN code for access. With advanced security procedures, this process was changed in later years to allow a user access through the fingerprint device without a PIN.

The pilot programs ran over the course of a year to test various devices (facial recognition and fingerprint) in different areas of the airport. The airport decided on fingerprint biometrics over facial recognition due to the poor performance of facial recognition, which was an immature technology in 2004/2005.

Once the device was selected and a deployment program determined, the time to procure the devices and cards was several months. An infrastructure upgrade was conducted concurrently with planning the card re-enrollment and biometric device deployment.

The system was procured under an existing security managed services contract with a vehicle to provide additional services. The managed service provider delivered a turnkey solution with costs for delivering the program and any associated recurring costs.

All hardware and infrastructure required to support the biometrics system required upgrades. To accommodate the new technology, both airports had to add a fiber backbone infrastructure, including modems, provide a continuous network backbone to system users, and upgrade existing access control loops/channels from leased lines or RS232 to RS422 fiber modems to communicate with the access control field panels. Future access control panels will also have the capability to use RS485 or TCP/IP protocols to communicate with the host via the fiber backbone.

The access control system vendor also required upgrades and new readers. The vendor performed some development work to ensure the new devices and badge media were compatible with the upgraded access control system. The vendor also updated the application to allow for biometric enrollment and smart card badge printing.

Smart cards were chosen based upon the following three primary factors (in order): Compatibility with the access control system, availability, and pricing. The new badge media is a multifunctional card that includes both the existing magstripe and smart card technology.

ENROLLMENT AND TRAINING

The credentialing office began communicating the changes associated with the new biometric system and smart cards with the airport community through Authorized Signatories and airport divisions. They also posted signs in the main ID Badging Office.

The biometric device vendor and the access control system vendor trained the managed service provider, who in turn provided training for all airport internal teams in the credentialing office.

The re-enrollment process started in 2006 with the first airport re-enrolling almost 40,000 badge holders as part of a 24/7, ninety-day program, and the second airport re-enrolling over 7,000 badge holders as part of 10/5 program in sixty days. The airport fast tracked the re-enrollment versus re-enrollment through attrition to meet internal schedules, as well as to use the opportunity to revalidate all badge holders in the system.

USER ACCEPTANCE

Acceptance efforts started with constant communication of the upcoming changes along with expectations. User acceptance was generally positive, with only a small number of people opposed to having their fingerprint captured. At the time of deployment, biometrics devices were not common, and many people did not understand exactly what data was being captured. For the concerned cardholders, the re-enrollment team took the time to explain authentication versus identification, as well as how data was being stored and captured. There were a few badge holders who still chose not to enroll in the program and their badges were cancelled.

COST CONSIDERATIONS

The airport did not consider a change in access control system vendor due to high satisfaction with the current system and the prohibitive cost of a total replacement.

There were new recurring costs to be considered and reviewed as Total Cost of Ownership:

- Biometric enrollment devices at the badging workstations
- New badge printers capable of printing smart cards
- Infrastructure upgrades
- Expedited enrollment process that required additional badging operators
- Continual purchase and replacement of smart card badges

SYSTEM RELIABILITY

Initially, the device threshold for an acceptable enrollment sometimes differed from the acceptable threshold of the field devices. This took some time and troubleshooting to correct and document the required threshold at enrollment and field devices.

Daily reports were run on both the enrollment process and field use to stay in front of any potential issues (enrollment success/fail rates, access grants/denies at biometric readers, etc.).

Enrollment Errors were posted for badging operators to understand and manage. These included “Bad Quality of Fingerprints,” and “Buffer overruns,” where the stored size of template is larger than the smart card will hold. These errors and others were also reported to the application vendor to remediate and provide code updates to be handled internally.

FUTURE PLANS

The airport is currently changing their fingerprint device to take advantage of improvements in pricing, technology, performance, and maintenance. Now that facial recognition is a more mature technology, the airport is again considering this as an option, but is waiting on case studies from other airports deploying facial recognition technologies.

A.6. Iris/Fingerprint Biometric for Access Control (Canada)

OVERVIEW

In 2004, the Canadian Air Transport Authority (CATSA) initiated the implementation of biometric-based access control for restricted areas in the nation's airports. This was done through the promulgation of nationwide regulations that created a Restricted Area Identity Card (RAIC).[106] RAICs allow access privileges that are roughly equivalent to the access control, background checks, and identity management requirements for unescorted access at US airports that are outlined 49 CFR 1542.207 to 1542.211.

The Canadian structure is like the US structure in that actions seeking the issuance of an RAIC are initiated through an individual airport. The airport makes the determination regarding which access portals an individual is allowed to enter. The airports supervise the submission of RAIC applications and, if approved, create and encode the cards for use with their access control systems.

The principal difference in the US and Canadian systems is found in the role of CATSA. In the US, unescorted access privileges are only registered at the airport level. In Canada, CATSA maintains a biometric-based central registry of all persons with RAIC privileges. This central registry has parallels with the Transportation Workers Identification Card issued for some US transportation workers. Additionally, the RAIC program managed by CATSA also requires that Class 1 and Class 2 airports (the nation's twenty-nine largest airports) operate enhanced access control at initial entry points into the restricted areas. The enhanced access control includes the use of fingerprint or iris biometric verification. No such specification for biometric-verified access exists in the US. It should be noted that US airports lobbied against a centralized identity database when it was raised by TSA at about the same time as Canada's was created.

SYSTEM DESCRIPTION

The major aim of CATSA's RAIC program was to afford enhanced security for access into restricted areas of airports. The architecture of the system is outlined in the Canadian Aviation Security Regulations. The schema can be characterized as centralized control over identity management and decentralized control and execution of access control functions. The centralized control feature involves the creation of a single identity database for all aviation workers who are afforded unescorted access to restricted areas of an airport. Any individual accessing a restricted area at an airport is required to have an RAIC. While the issuance of a RAIC occurs at the airport, it requires CATSA authorization based on the submission of a fingerprint biometric. That fingerprint biometric is linked to a CATSA Identification Number (CIN) that ensures that an individual can only have one RAIC at any given time.

In some cases, an RAIC credential can have privileges added at another airport if that airport determines such privileges are required. However, there is never more than one RAIC issued. The airport that issues an RAIC is responsible for recovering the RAIC once access privileges are no longer required. If the RAIC holder is afforded privileges at another airport and the initial issuing airport deactivates it, a new RAIC will have to be created by the airport if privileges are to be continued.

The CATSA system uses both fingerprint and iris biometrics in connection with its access control systems. The fingerprint biometric serves as the identity marker, and is recorded in the centralized

[106] **Canadian Aviation Security Regulations SOR/211-318:** https://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-318/FullText.html

CATSA system before the CIN is issued; the fingerprint is also used as an identity authentication marker encoded on the RAIC. The iris biometric is only encoded on the RAIC as an authentication marker.

In addition to administering the centralized registry for the RAIC program, CATSA provides the hardware and software for biometric access control, including cards and printers for RAIC issuance.

In most instances, interior access points are equipped with both iris and fingerprint biometric readers. These readers are generally located in mantrap or sallyport areas that lead into an airport's restricted areas. Some locations, like outdoor gates, are equipped solely with portable fingerprint readers.

When an RAIC holder seeks access, they present the RAIC, and the reader performs a 1:1 match between the biometric presented and the template of that biometric stored on the RAIC. Where an access point is equipped with both iris and fingerprint readers, the RAIC holder may present their card to the reader of their choice.

At RAIC issuance, the biometric templates are created and encrypted on the RAIC. The airport does not keep copies of the biometrics or the templates on their systems. Once the templates are successfully encrypted on the RAIC and tested, the airport is required to discard the templates. Limits on biometric data use and retention are clearly provided for in governing legislation.

PLANNING AND SELECTION

CATSA was responsible for planning and rolling out the program consistent with regulatory requirements. Planning for the centralized national system began in 2004, two years after the agency was established.

CATSA created working groups to plan the RAIC process and address implementation issues. The working groups included participation from Transport Canada, air carriers, airports, unions, and other aviation sector stakeholders. The working groups addressed a range of technical and security issues as the RAIC program was formulated. The focus was on building a common architecture for the national program that could integrate with existing access control systems.

As part of the planning, CATSA evaluated and selected fingerprint and iris readers that would support the program and integrate with a variety of existing access control systems at the nation's airports. They looked to users of technology inside and outside of the aviation sector to select hardware and software for system operations.

With respect to selecting a fingerprint technology, CATSA referred to experiences of organizations including the US Army, NASA, American Express, the New York Police Department, and Continental Airlines. The planners considered Weigand communication and the capability of the system to communicate with existing proprietary and non-proprietary access control systems.

Regarding the iris biometric, CATSA examined the experiences of Schiphol and Frankfurt airports, which had deployed iris verification technology on ramps and tarmacs. Systems were assessed to evaluate their compatibility with proximity and smart cards.

CATSA also evaluated card technology to identify suitable card stock to support the program. This included ensuring card memory was sufficient to store two biometric templates, as well as considering compatibility with magnetic stripe and prox card technologies.

DEPLOYMENT

While the RAIC system is part of a centrally controlled identity management program, the installation and operation of the hardware and software is performed at the local airport level. All airports were included in the RAIC program, but only the busiest were selected for enhanced biometric access control (all Class 1 and 2 airports, and a few Class 3 airports).

A pilot program was conducted in 2004 at four airports involving approximately 40,000 RAIC holders. The full rollout of the RAIC program occurred over two years for all twenty-nine airports utilizing biometric access control, concluding in 2006.

PROCUREMENT

CATSA is responsible for the procurement of all hardware and software relating to the RAIC. The labor required for preparation of the RAIC is the responsibility of the local airport. Where the biometric access control units are utilized, those units are provided by CATSA and installed by the airport.

ENROLLMENT

As noted above, the airport manages the application and enrollment process for persons seeking restricted area access at their airport. That process starts when a person is sponsored by an airport or associated company. Information about the individual is submitted to Transport Canada to run a security check. A biometric fingerprint template is taken and submitted to CATSA so that its identity database can be queried to determine if an active RAIC has been issued to someone who matches that biometric. If no match exists, the applicant will be issued a CIN and an RAIC card can be issued.

Once the airport receives security approvals from Transport Canada and authorization from CATSA, the RAIC can be created and issued. At the airports where biometrics are deployed, issuance includes encoding the card with biometric templates for fingerprint and iris to work with biometric access control readers. It also includes encoding by the airport with respect to the access points at which the RAIC can be utilized. Those decisions are the airport's alone.

If the RAIC holder is granted privileges at another airport, the card can be encoded by that airport to grant access. However, if the airport that initially issued the card deactivates it, the RAIC holder will have to apply for a new card through the second airport. The issuing airport is responsible for inventorying and tracking the cards it uses until it deactivates those cards.

At the time of issuance, the card is tested to ensure that the biometric templates are properly encoded. During iris enrollment, individuals are encouraged to remove eyeglasses, though eyeglasses need not be removed when seeking access. While a small percentage of enrollees had unreadable fingerprints there were no reports of unreadable iris. Accordingly, the dual system means that every person is able to use some form of biometric, and in most cases both forms.

Once testing of the biometric is completed, the airport deletes the biometric template information from its database. The template data is only stored encrypted on the card. Renewals and reissuance of damaged or lost RAIC cards are handled by the issuing airport.

USER PREFERENCE

The airport interviewed experienced little user resistance to the introduction of biometric authentication measures.

The airport indicated that, where both biometric access control measures were present, about 70% of the user population chose the fingerprint biometric and 30% chose the iris solution. The airport operator noted that this was roughly the same use breakdown before, during, and after the pandemic.

Some users expressed concern over lasers in connection with use of the iris solution, but those concerns were debunked. The airport operator believes that the preference for fingerprint is generally attributable to greater familiarity with that solution and personal preference.

EFFICIENCY AND EFFECTIVENESS

It was noted that portable fingerprint readers utilized at outdoor locations were bulky and less efficient than their indoor counterparts. These wireless devices require twice daily download of template data.

The airport interviewed noted the following challenges relative to the iris biometric system:

- The readers are not outdoor rated
- The readers have some sensitivity to lighting conditions
- Enrollment requires the removal of eyeglasses

The following challenges relative to the fingerprint biometric system were noted:

- There is a significant population with unreadable fingerprints
- The system have reduced performance in inclement weather

SYSTEM RELIABILITY AND MAINTENANCE

CATSA noted that the fingerprint reader, as a touch-based system, requires regular routine cleaning of its sensor head. Conversely, the touchless iris system does not require regular cleaning. However, unlike the facial system, the fingerprint system is outdoor rated and reported to be less sensitive to environmental conditions.

No reliability issues were noted with respect to the hardware or software for the iris biometric solution. The fingerprint readers did have some coil issues attributable to the high level of use. Generally, the systems were presented as comparable. CATSA handles unit replacements.

No data was available on the false acceptance rates or true acceptance rates of either biometric solution. However, the airport interviewed observed that both systems seem to function comparably. The iris biometric does cycle faster, but the speed of use was more a function of the user’s ability to present their biometric than the ability of the reader to process the data. The iris biometric also has some adjustability when capturing to account for height and user position. In the opinion of the airport operator interviewed, errors denying access are most often the result of employees failing to present their biometric properly. Both biometric solutions are positioned to accommodate persons with disabilities.

In some cases, lighting conditions interferes with the ability to use iris biometrics. Also, those readers are not ruggedized and cannot be utilized at outdoor access points.

APPENDIX B: PASSENGER JOURNEY CASE STUDIES

To enhance efficiency and security, airports are increasingly turning to biometrics to transform the passenger journey. Examining the biometric applications for passenger journey currently in use at airports also offers important lessons on the possible implementation models.

The implementation of biometric systems at airports comes with considerations and challenges like that of access control systems. Issues such as privacy concerns, data protection, and the need for secure storage and transmission of biometric information must be addressed to ensure public trust and regulatory compliance. Collaborative efforts between airport authorities, airlines, and technology providers are essential for developing standardized protocols and ensuring the responsible and ethical use of biometric data.

B1: Curb-to-Gate Solution Pilot – This case study describes a major airline's introduction of a Curb-to-Gate biometric passenger journey to an airport after testing the concept at other US airports. The airline led the implementation team in coordination with TSA, CBP, and airport stakeholders.

B2: Biometric Bag Drop – This case study reviews biometric bag drop processes operated by two major airlines at one airport. The two projects had significantly different levels of airport involvement.

B3: Biometric Common-Use E-Gate – This case study details an airport's efforts to develop common-use, an automated biometric gate solution, with a focus on improving the passenger processing experience, enhancing security, and increasing operational efficiency. The airport's approach recognized that the integration of multiple air carriers into a single, common-use platform necessitated a flexible solution capable of meeting each carrier's needs.

B.1. Curb-to-Gate Solution Pilot

OVERVIEW

This CAT X airport is owned and operated by its city of residence. It is the major hub for three airlines and hosts many international carriers.

A major airline introduced the Curb-to-Gate Biometric Passenger Journey to the airport after testing the concept at other US airports. In coordination with the TSA, CBP, and airport stakeholders, the airline led the implementation team.

The project objectives addressed the airline and airport's shared desire to improving customers' curb-to-gate experience by streamlining bag drops and document-control processes. In addition, the digital management system requires less personnel to facilitate customer movement through the various touchpoints on their journey to airport gates.

PROGRAM DESCRIPTION

The Curb-to-Gate Biometric Program is a digital identification management system that employs facial recognition technology to allow passengers to drop their bags at airline checked bag stations, access TSA document control stations at checkpoints, and enter airline-controlled aircraft departure gates. This is a proprietary system that requires passengers to download the airline app on their mobile device, be enrolled in the TSA Pre-Check Program or CBP Global Entry Program, and have a registered Known Traveler Number in their airline passenger records file. A third-party agency interfaces airline passenger record numbers (PRN) with digital images contained in TSA/CBP known traveler databases for use in the digital management system. When checking in on a mobile device, passengers may opt in to the digital management system for access to the Curb-to-Gate Biometric System.

The airport provided infrastructure for the system through airline lease agreements. Passengers may use the airport Wi-Fi system to access the airline's app.

Bag Drop

A ticket counter area in the terminal's lower level was converted to the Digital Management System Bag Drop site. Customers access this area from the lower-level curb. The bag drop facility has four processing stations consisting of a facial recognition digital machine, baggage tag machine, and an intake belt.

Currently, the digital facial recognition process begins automatically. If the system detects a match between the presented individual and the system database, a bag tag is issued to the individual. The passenger places the tag on the bag and places the tagged bag on the intake belt. Passengers may check multiple bags during this process. However, the system is programmed to reject PRNs that include more than one individual in the same travel record. The airline and TSA are considering a workaround to address this issue.

Security Checkpoint

The journey continues through TSA's document verification and screening at the passenger security screening checkpoint. The airport has a designated checkpoint segmented into TSA PreCheck, digital facial recognition, and CLEAR entry lines. Customer service agents direct the digital facial passengers to a single line for access to the digital facial management system. Passengers approved for digital facial access are not required to present identification cards or travel documents at the verification station. If the system matches the passenger's facial image with the data contained in the individual's CBP Passport Digital Identification files, the passenger proceeds through the document control station.

Boarding

Selected gates are equipped with digital facial readers/cameras. Gate agents must turn on the camera to allow passengers to use facial recognition for access to the boarding gates. Due to the limited deployment of these cameras, passengers must indicate that they would like to use facial recognition instead of a boarding pass or electronic device. Currently, digital identification is not widely used at the boarding gates.

B.2. Biometric Bag Drop (Airport and Airline Initiatives)

OVERVIEW

This CAT X airport has two biometric bag drops, which are operated by two major airlines, A1 and A2. Those projects had significantly different levels of airport involvement.

- A1 – The airport was interested in piloting biometric technology in passenger journey, and A1 agreed to work with the airport to look at bag drop applications. A1 and the airport outlined the features and functions most valuable to the airport. The airport took a lead with respect to identifying airport concerns and desires and working to help shape the A1 initiative to meet airport objectives. The A1 initiative was handled as a pilot with significant involvement by the airport. The airport was involved in baselining performance of legacy systems before the project was initiated.
- The airport took a more hands-off role with respect to the A2 project as the airline already had a process in place. The airport was not involved in collecting baseline data, and while the airport has made some operational suggestions to A2, the operation of the biometric bag drop is a standard approach that is similar to A2's operations in other airports.

The airport indicated an extensive number of stakeholders were involved in the projects, including airport Innovation, Airline Relations, Legal, Procurement, IT, and Operations departments; airline customer service and training departments; external product and innovation firms; baggage handling service providers; and regulatory partners.

The airport maintains an office dedicated to innovation, as well as employees dedicated to customer satisfaction and experience. Additionally, the airport maintains a strong internal IT services department to support technology issues. In addition to these service resources, the airport has well-staffed security and facilities sections to support these types of initiatives.

It was noted that A1 anticipated that the biometric bag drop process would reduce the resources requirement for airport personnel when TSA began acceptance of the biometric identity card check. At that point one person could manage four baggage drop positions.

SYSTEM DESCRIPTIONS

A1 System

The A1 data system matching required the presentation of a government ID in connection with the process.

- The system was operated as a pilot program jointly sponsored by the airport and one airline.
- The pilot was never expanded to a phase where the individual did not have to present their government ID to an airline employee supervising the bag drop.
- The bag drop transaction occurred at a baggage counter monitored by airline personnel.
- The pilot was designed to inform future tests of touchless technologies.

A2 System

The airport described the A2 bag drop process as follows:

- Guests tag their own bags after checking in at the kiosk, and then proceed to the automated self-bag drops
- Guests are advised of the biometric option after scanning their boarding pass at the self-bag drop; They may either opt in and continue unassisted or opt out for agent-assisted service

- Once the guest opts in, the unit instructs them to scan their ID on the built-in hardware
- The unit compares its scan of the photo on the ID with a facial scan captured by its on-board camera, and compares the ID information with the guest's reservation details
- Upon a successful match, the guest places their bags on the conveyor belt attached to the unit, which scans the bags, weighs them, accepts payment for any additional services, and sends them to the checked baggage system

The airport reported that the A2 system processes 400–500 bags per day.

Media reports indicate that the A2 system is the same as the airline's systems in other airports. Those reports indicate the system can accept over 50,000 forms of ID from over 200 countries.

LEGACY SYSTEMS COMPARISON

In preparing for the A1 pilot, the airport did extensive measurements of existing processes to verify the pilot program results. The comparison between the legacy and the A1 system did not demonstrate significantly improved process efficiencies. Additionally, a more robust analysis that considered other factors such as emotional response to the new system provided mixed results. The airport opined that human engagement in the process might have value that is lost with a full biometric solution. The airport was also not convinced that the A1 pilot met its objective of a unique passenger experience.

Evaluation of the A2 experience was more limited. The airport was not involved in baselining prior to implementation and had less input in the system design. The project was designed to meet A2's requirements with less airport input. Testing data from a deployment of the A2 system at another airport was reported to reduce passenger processing time to seventy seconds, representing a 30% reduction in processing time.

DEPLOYMENT

With respect to integrations, the challenges were primarily with the A1 system's integration with the airport systems. The airlines selected the software platforms. In the case of A2, one vendor provided the hardware, software, and integrations; with A2, there were no links to any systems.

The A1 system integrations to the Departure Control System and Baggage Handling System were performed by another vendor.

In contrast to the A1 deployment, the airport had little involvement in the process deploying the A2 system. That deployment seemed to follow the airline's already developed process that was being applied simultaneously at several other airports.

The security checkpoint and gate operations are not linked to either airport's bag drop operation.

No infrastructure challenges or impediments to implementation were identified. The airport industrial engineers addressed passenger flow issues, provided inputs on technology, and identified design flaws in supporting equipment.

DATA COLLECTION

The A2 baggage drop system collects the information necessary to link the passenger to their luggage. In addition, the biometric sensor collects image data that validates the image on the government-issued ID matches that of the individual in front of the biometric sensor. The biometric verification data is shared with the TSA for audit purposes only. Currently, the airport does not access that data, though they are not ruling out the possibility of seeking limited access in the future.

The bag drop does collect personal information related to passenger record data of individuals utilizing the bag drop equipment. The airport currently receives anonymized aggregate reports about use of the system. This information gives insights about the use of the bag drop systems as well as traveler movement through the airport.

The airport also conducts behavioral analysis to ascertain the emotional reaction of passengers to the biometric equipment and processing. That type of analysis requires significant commitment of technical expertise and resources.

B.3. Biometric Common-Use E-Gate

OVERVIEW

This CAT X airport was a pioneer in the application of biometrics to expedite passenger processing. The airport operates nine terminals, including eight domestic and one international, which have a total of 128 gates. To support its extensive international air carrier operations the airport also created a midfield satellite concourse (MSC) to expand the operations of its international terminal. The combined international terminal services over thirty-one international air carriers, with the MSC adding an additional eighteen gates that are used by a mix of international and domestic carriers.

The airport's efforts with respect to biometric technology focus on improving the passenger processing experience, enhancing security, and increasing operational efficiency. In doing so, the airport sought to use touchless biometric technology in its passenger processing by leveraging the CBP's US VISIT exit monitoring program. While the initial focus was on the international travel experience, the program was designed to enable expansion into the domestic travel operations as well.

The airport's approach recognized that the air carriers have significantly different capabilities and appetites for biometric application. The integration of those air carriers into a single common use platform with automated biometric gates (ABG) necessitated a flexible solution capable of meeting each carrier's needs. Accordingly, the system needed to be designed and operated with the capability of meeting the processing requirements of air carriers who had not yet embraced biometrics. It also anticipated scalable expansion into domestic operations if, and when, biometric processing was accepted there.

PLANNING AND PROCUREMENT

The airport began efforts to implement biometrics in passenger processing in 2017 when it conducted a pilot project in conjunction with two air carriers. The pilot involved equipping a limited number of international departure gates with facial biometric solutions to facilitate the US VISIT exit monitoring requirements, and to expedite the passenger boarding process. Based on the pilot testing, the airport sought to implement an airport-sponsored, common-use, ABG solution.

A detailed RFP was facilitated by the experience of the initial pilot. The airport released an RFP in April 2019 seeking ABG solutions. It initially planned to install fifty-two ABG units at fourteen gates. In addition to those plans, the airport was looking for potential expansion to an additional forty gates with up to 160 ABGs in other terminals.

The use of ABGs in a common-use platform required the airport to design and implement a system capable of working in different modes to accommodate diverse air carrier requirements. Where the air carrier was unable to interface with the ABGs, the common-use platform had to be capable of operating as self-boarding gates, utilizing traditional barcode scanners for electronic and paper boarding passes.

The RFP required the proposer to submit methodologies for the development of plans to integrate and test the systems and to train users. The RFP also specified testing requirements, including specifications for both demonstration and final testing. Additionally, the RFP required the establishment of training programs for airport staff and air carrier personnel.

The core planning and implementation partners for the project included:

- Airport staff
- Common-use system provider
- ABG manufacturer

- Biometric equipment provider
- CBP
- Contracted IT support company

The group worked closely with the participating airlines to ensure that the ABG could accommodate the requirements of each air carrier's departure control system (DCS), while at the same time meeting CBP requirements.

As part of the planning process, the airport offered informational briefings and prepared informational materials for the air carrier partners.

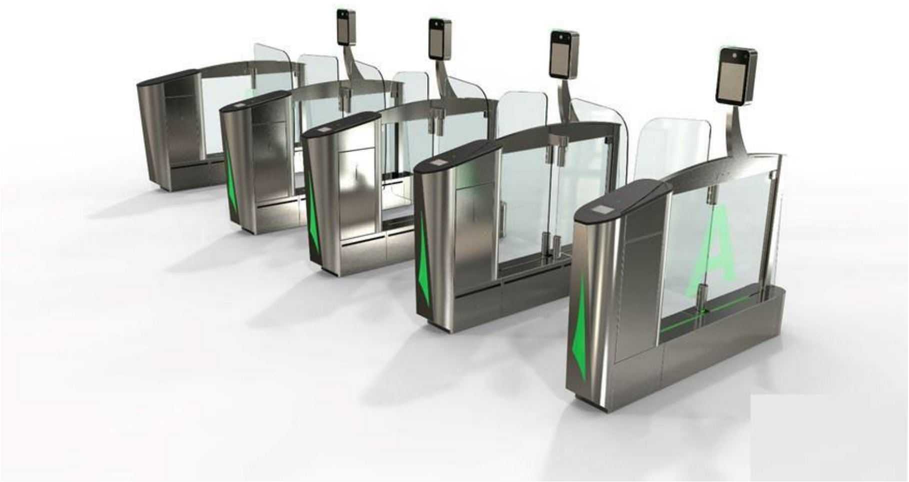
The airport was looking into the operation of this ABG system utilizing the Software-as-a-Service model. IT envisioned service level agreements with the proposer for purposes of system operation.

Construction was supervised by the airport but managed as part of the overall project plan by the proposers. In accordance with the RFP, detailed project schedules were created outlining construction activities. The RFP also required the proposer to coordinate with relevant airport staff regarding construction activities.

SYSTEM DESCRIPTION

The ABG system's hardware components include the gates, customer service podiums, and camera systems that capture images and transmit data to the TVS. These hardware systems also have software components that need to be integrated into a common-use platform. The common-use platform had to be capable of integrating with all the ABG operating systems, CBP's TVS, and the DCS of each air carrier. The RFP required the successful bidder to provide all required hardware and software to support the ABG installation and operation within a single common-use platform.

Figure B-1. Automated Biometric Gate Solution (ABG)



Within the common-use platform, the ABGs can operate in different modes, including:

- As an automated biometric gate using biometric face match only (One-Step Mode)
- As an automated biometric gate using face match and a boarding pass scan (Two-Step Mode)
- As an automated self-boarding gate utilizing a boarding pass scan only (Traditional Mode)

As of June 2023, ABGs with biometric capabilities are only being used for international flights.

The three-mode configuration of the system allowed the ABGs to interface with the DCS of all carriers. In the Traditional Mode, the passenger simply scans the boarding pass, and the required identity verification is conducted by airline personnel. It operates as a self-service gate that checks the validity of the boarding pass and regulates access. It performs no identity verification function.

In Two-Step Mode the passenger scans the boarding pass, and the camera captures an image. The ABG submits required data to the CBP TVS. The boarding pass data is held until TVS matches the image. If the TVS determines a match, the boarding pass data is forwarded to the airline DCS to determine whether the passenger is clear to board. If there is no TVS match, the passenger is directed to an agent.

The One-Step Mode can only be utilized by passengers within the context of the US VISIT exit program, which only applies to international flights. As the passenger approaches the gate, the camera captures their facial image and passes it directly to CBP's TVS. TVS responds by transmitting unique identifying information to the airline's DCS through the common-use platform. The airline DCS then can notify the ABG that boarding is authorized. This method is touchless, requiring no presentation of boarding pass information.

The multi-mode design of the ABG's allows air carriers to move to a biometric process when they develop biometric capabilities.

The program began with installation of ABGs in the newly constructed MSC, which was greenfield construction. The program subsequently moved to the decommissioning of existing passenger processing technology and installation of the ABGs in the legacy portions of the international terminal. That work required demolition of the existing gates and podiums, restoration work, and new installation.

While the biometric program is not currently linked to check-in or bag-drop programs, those integrations are under consideration. The eventual goal is a curb-to-gate solution.

Technical Requirements
The technical requirements for the ABG systems outlined in the RFP were extensive. They began with a summary of points regarding design and installation expectations including:

- Full integration with the airport's common-use system
- Configuration to support gate operations for multiple air carriers
- Support for the use of all boarding applications
- Technology to facilitate biometric capture of international passengers subject to US VISIT exit requirements
- Integration with CBP biometric programs including TVS (these requirements were detailed in an appendix)
- Firmware, software, and hardware elements certified to operate successfully in and maximize the flexibility of the common-use system
- Operational flexibility for automated or manual air carrier operations
- Automated collection of performance metrics to support airport data analytics, business intelligence, and operational awareness. Required metrics specified for capture on a per flight basis were:
    - Number of passengers scanned
    - Transaction counts
    - Transaction times
    - System fault reporting

- Capability for ABG operation in One-Step, Two-Step, and Traditional Modes
- Capability to expand to domestic terminal areas

The technical specifications also addressed:

- Software requirements-including upgrades, updates, and patching, as well as preferred operating systems
- Security of information and applications meeting requirements set by CBP, TSA, FAA, and the airport
- Development and execution of information security programs and practices composed of:
    - Security controls
    - Security design and review measures
    - Plan documentation
    - Security Assessments (based on ISO standards)
    - Security Issue remediation measures
    - Cloud security measures (including a range of cloud provider security requirements)
- Functionality requirements for ABG equipment addressing:
    - General characteristics of equipment to be provided
    - Physical specifications (designed to prevent unauthorized access)
    - Boarding Gate Reader requirements
    - Biometric camera requirements for quality, capture on approach to the ABG, and for “stacking” of families travelling together
    - Alarms for detection of unauthorized access activity (including audible alarms)
    - Battery backup
    - Emergency opening provisions

The detailed RFP allowed the airport to select a team of experienced vendors capable of meeting the project’s equipment and design requirements.

The ABG’s biometrics process utilizes a 1:N match against a limited TVS gallery of persons prepared by CBP. The TVS gallery includes images of individuals scheduled to travel. The data matching occurs in the following process:

- Seventy-two hours prior to an international commercial flight’s departure, the air carrier will provide CBP with a flight manifest that includes relevant passenger information and a unique identification designator generated by the airline
- As the departure time approaches, CBP in its TVS system will create a gallery of images of passengers on the manifest for the flight from their biometric information records
- At the boarding gate, ABG’s software will establish a secure internet connection with CBP’s TVS
- When boarding is ready to commence, the ABG will report the flight number to TVS
- As a passenger enters the ABG lane, a facial image is captured and sent to TVS. TVS will conduct the matching against biometric information in the gallery and respond to the ABG regarding whether a match was established

- Where the airline has created a unique identifier (UID) for passengers and noted it on the manifest (required for One-Step Mode processing), that UID will then be provided back to the airline to confirm the associated passenger's boarding status.

The design of the ABGs affords the air carriers the ability to adapt their operations over time. It also provides a technology platform that allows the air carrier time to migrate their DCS systems in a gradual fashion.

DEPLOYMENT

The deployed ABGs operate as a part of a software-as-a-service model, with a private provider managing the hardware and software for the installed ABGs in accordance with service-level agreements.

Initially, twenty-four ABGs were deployed at six gates in the MSC. Once the ABGs in the MSC were successfully installed, a plan was developed for implementation in the legacy areas of the international terminal.

The most significant challenge noted was integration with TVS. CBP published "U.S. Customs and Border Protection Biometric Air Exit Business Requirements," outlining the process and specifications for integration with TVS. Those business requirements were directly incorporated into the RFP, and formed the basis for the biometric collection and use by the ABGs. The common-use system needed to adapt to CBP's TVS requirements, and the air carriers then needed to adapt their DCS to integrate with the common-use system.

The air carrier integration required development of solutions based on the capabilities of each carrier's DCS. Because the ABGs can be operated without biometrics in a Traditional Mode, integration of biometrics was not required before ABG deployment. However, if those air carriers decide to use a biometric process in the future, or if the use of biometric is subsequently mandated by CBP, air carriers currently operating in Traditional Mode will require further integration.

The airport is actively educating carriers on the advantages of full biometric integration. This includes educational programs for air carrier personnel at the airport as well as communication with the corporate offices. Those programs include an outline of the technical integration with the airport's common-use platform.

In addition to external integrations, the ABG system's hardware and software components needed to be integrated into the common-use system. To conduct that integration, the airport sought vendors that demonstrated experience in the deployment and operation of each of the component parts of the program. The team selected for the ABG included firms with national and international experience designing and operating common-use systems, biometric identity management systems, and automated and biometrically enhanced e-gate systems.

No infrastructure challenges or impediments to implementation were identified. The ABG proposer was responsible for securing all required construction and other permits. With respect to projects in the international terminal, the decommissioning of existing equipment to make room for the new ABGs was also required.

The airport has not noticed any difficulty in passengers adapting to the new processes. Signage is posted at the gates notifying passengers of their opt-out rights. However, the airport reports that few passengers choose to opt out, and most passengers like the convenience of the ABGs.

DATA COLLECTION

The biometric data captured and processed at the ABG is not shared with the airport or airlines or retained in the ABG systems. It is passed directly to the CBP's TVS through a secure internet connection, and is then analyzed by the TVS in the cloud. The only information shared with air carriers is the same type of passenger data currently available in the DCS. Currently, US citizens can opt out of biometric data collection, even on international flights involving US VISIT exit procedure. The airport is required to post signage advising passengers of the right to opt out.

The ABGs collect non-PII, statistical data relative to passenger processing. This includes numbers of passengers processed with dates and time stamps. That information is provided by the ABGs to the airport's designated internal data systems.

DATA MANAGEMENT

Storage of biometric data by the airport and air carriers is prohibited by the CBP TVS business rules.

The airport has reserved the right to collect and maintain non-PII, statistical data from the ABGs. The ABGs are required to have a system to delete data roughly every thirty days. There is no specified limit on how long the statistical data can be maintained by the airport.

The RFP specified technical and programmatic measures to ensure security, demonstrating the concept of Privacy by Design. These privacy measures require the posting of signage and opt-out processes.

Consistent with the "U.S. Customs and Border Protection Biometric Air Exit Business Requirements," the airport is required to apply the FIPPs to data collected for TVS.

Privacy protection measures include technological measures to protect data security and process measures to protect biometric data. The biometric data is encrypted both at rest and in transmission to the TVS. Data matching is conducted by the TVS in the cloud. Boarding-related information is only returned to the air carrier from the TVS utilizing a specially created UID.