Transportation Security Administration

TSA IDENTITY MANAGEMENT ROADMAP

For Transportation Security and the Credential Population and Passenger Experience

February 2022

TABLE OF CONTENTS

Administrator's Message

January 24, 2022

Since its inception, the Transportation Security Administration (TSA) has been dedicated to protecting the Nation's transportation system to ensure freedom of movement. Identity management (IDM) ensures the right people have access to the right transportation infrastructure areas at the right times. IDM is critical to TSA's mission, but it is also imperative for the credential population and passenger experience. The IDM Roadmap builds on the work of our Biometrics Roadmap (2018) by articulating a comprehensive end-to-end strategy for IDM at TSA and chronicling the next iteration of TSA's thinking on biometrics. This Roadmap will serve as the blueprint for future IDM work across the Agency and addendums will be published to expand on emerging priority topics.

As we explore solutions to meet the goals and objectives identified in this Roadmap, it is important that we think toward the future. Technology like digital identity, artificial intelligence, machine learning, and block chain present new possibilities for efficient and effective IDM solutions. We must continue to identify innovative solutions that allow us to improve IDM while mitigating risks to our transportation systems.

I want to thank everyone at TSA and our industry and interagency partners who had a hand in creating this Roadmap, as well as all those who work to achieve its goals each day. Together, we will make its vision a reality and continue to achieve the high expectations of the traveling public, our stakeholders, and each other.

Sincerely yours,

David P Pekoske

David Pekoske
Administrator

EXECUTIVE SUMMARY

Identity management (IDM) ensures that the right individuals have access to the right resources, at the right time, and for the right reasons, in support of federal business objectives. IDM is necessary to TSA's mission to protect the Nation's transportation systems and ensure freedom of movement for people and commerce. Given the ever-evolving threat landscape, TSA has expanded its security focus from objects and method-threats (such as shoe bombs and liquids) to place an increased emphasis on the individuals that pose the threats. IDM is critical to ensuring TSA has confidence in presented identities and can mitigate risk across various transportation modalities.

For the Roadmap's purposes, IDM is defined as the process of (1) collecting an individual's information during credential enrollment or travel reservation, (2) confirming a person's identity using identity assurance leading practices, (3) maintaining confidence in that identity throughout evaluation (vetting) processes to assess that person's risk level, and (4) verifying the person's identity at access points such as airport checkpoints. IDM primarily works to ensure the safety and security of transportation spaces by confirming and maintaining confidence in a presented identity throughout the entire IDM lifecycle.

Previously, the IDM functions (enrollment and reservation, identity proofing, vetting, and identity verification) were managed separately, but TSA now approaches IDM as a holistic lifecycle. This Roadmap lays out TSA's overarching vision for IDM, as well as its supporting goals and objectives to guide capability development across the IDM lifecycle. This lifecycle effectively manages dynamic risk, while improving the credential holder and passenger experience and employing innovation to support the evolving needs of the Agency, its partners, and the traveling public. This vision will enable the Agency to iteratively build capabilities by automating manual processes where needed, preserving and scaling existing successful tools and technologies, and introducing innovative solutions across populations according to applicable laws, authorities, civil rights and liberties, and privacy considerations.

This vision is achievable by aligning and advancing the IDM lifecycle phases in the future state goals and objectives that are presented in **Figure 1.**

Figure 1: IDM Lifecycle 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

I. PURPOSE AND SCOPE

This Roadmap will serve as an evolving document that articulates TSA's guiding vision for IDM of credentialed populations and the traveling public. It will be used to guide innovative and creative solutions to meet the needs of changing technologies, evolving travel metrics, and shifting threat landscapes; as well as to scale successful efforts across the phases of the IDM lifecycle. The enrollment and reservation, identity proofing, vetting, and identity verification phases are defined in **Figure 2.**

The Roadmap's strategic vision and goals apply to all individuals looking to use a credential (physical or logical) or obtain access to transportation spaces, including populations illustrated in **Figure 3.** It applies to aviation, maritime, and surface transportation modalities and builds on the extensive processes and infrastructure already in place. Although this vision applies to both passengers and credentialed populations, many standards, requirements, and processes described in this document may apply differently to credentialed populations with access to transportation spaces and infrastructure. IDM processes are applied based on population. They use a risk-based approach to make access decisions based on the risk posed to transportation spaces and information.

As TSA develops and scales new and existing solutions to meet evolving needs, it will do so consistent with its authorities, while adhering to laws and regulations that protect the civil rights and liberties and privacy of passengers and credentialed populations. Privacy protections will continue to include restrictions to prevent the use of applicant and passenger data for purposes other than transportation security. TSA adheres to government information assurance standards to secure data. These standards help protect both applicants and passengers as well as the integrity of TSA systems across the data lifecycle.

Figure 2: Phases of the IDM Lifecycle

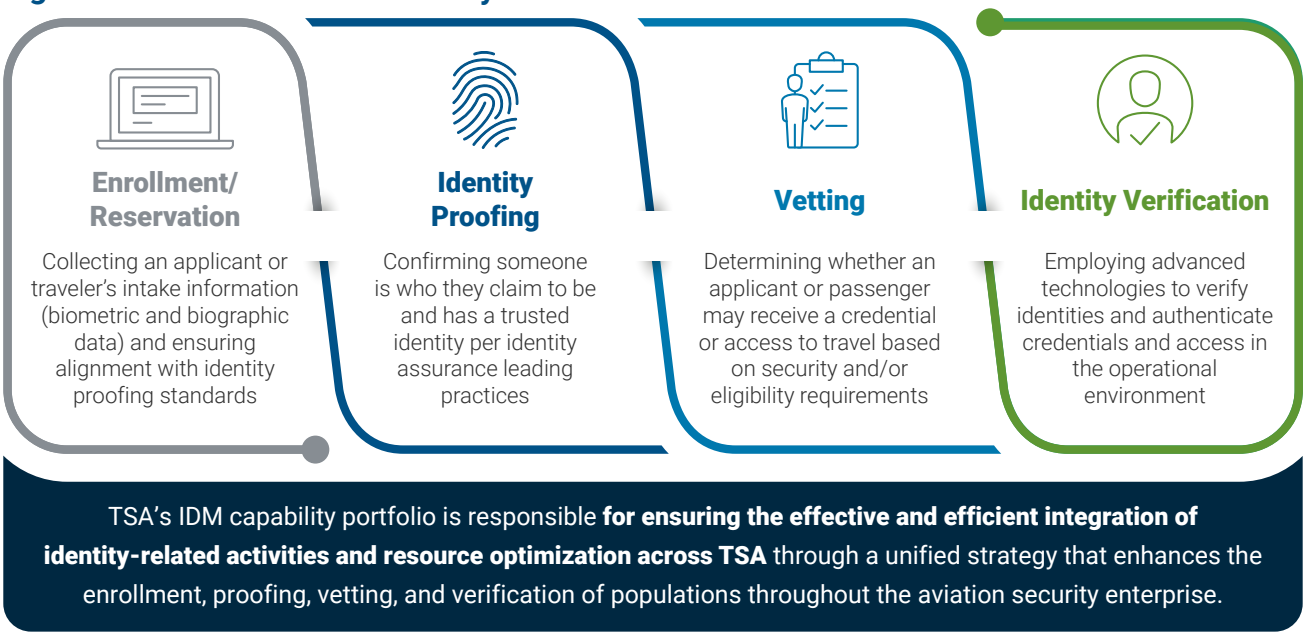


Figure 3: Population of Individuals Accessing Transportation Spaces

II. GUIDING PRINCIPLES

When designing the IDM Roadmap and its goals and objectives, TSA considered the overarching principles shown in **Figure 4.** These principles provide a set of considerations that guide TSA in its execution of the goals and objectives of this Roadmap and the solutions developed to achieve them.

Figure 4: IDM Guiding Principles

Risk Management

The Roadmap incorporates and enables the continued development of standards and frameworks to assess the risks posed by an individual or groups to provide cohesiveness across the IDM lifecycle and a risk-informed approach when granting access based on accepted risk standards.

Person Centric

A person centric approach is the positioning of processes around an individual's identity. It uses the information provided by individuals to evaluate the risk they pose to the transportation enterprise, including secure spaces and information. TSA also prioritizes opportunities to scale existing person centric functions and introduce new elements of human-centered design to improve the customer experience.

Privacy

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

Resource Optimization

TSA recognizes the vast amount of information that exists within TSA, the U.S. Government, and industry. In planning for the future, TSA will coordinate across these spaces to understand changes in risk, human behavior, travel patterns, and technological opportunities. In doing so, TSA will maintain the most up-to-date understanding of the evolving threat landscape and adapt policies and procedures throughout the IDM lifecycle.

III. IDM VISION

TSA will collaboratively and cohesively evolve the IDM capability that manages dynamic risk, while improving security effectiveness and the credential population and passenger experience, as well as employ innovation to support the future needs of the Agency, its partners, and the traveling public. As the threats posed to the transportation enterprise are evolving, TSA focuses on IDM based on the level of risk an individual poses to transportation spaces and information, in addition to physical screening.

Using a person-centric approach, the IDM ecosystem at TSA will work to stay ahead of changes in the threat landscape, continue to grant credentials and access fairly and accurately, and manage emerging threats throughout the enrollment/reservation, identity proofing, vetting, and identity verification phases. The phase-specific visions and key actions are further explained in **Figure 5**, which demonstrates the cohesive nature of the future vision of IDM at TSA.

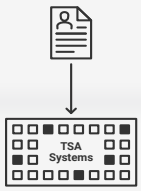
This future vision will enable the Agency and its partners to iteratively build capabilities by automating manual processes, preserving and improving existing tools and technologies, and introducing innovative solutions across populations according to applicable laws, authorities, civil rights and liberties, and privacy considerations.

Figure 5: IDM Phase-Specific Visions and Key Actions

Enrollment / Reservation

Vision
TSA seamlessly collects relevant applicant and passenger biometric and biographic data, based on the credential or access being provisioned, in alignment with identity proofing standards

Key Action
Individuals provide information (biometric and/or biographic) via enrollment and reservation platforms

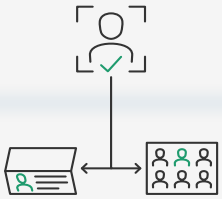


Impact
Expanded virtual enrollment options improve the accessibility and convenience of enrollment

Identity Proofing

Vision
TSA has a real-time picture of who a person is and can confidently assert that all individuals receiving a credential or access have a verified identity

Key Action
Applicant and traveler data is validated against internal and external TSA-trusted sources

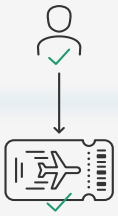


Impact
Automated tools minimize manual errors and reduce the amount of government and applicant interactions

Vetting

Vision
TSA continues to use identified leading practices and evidence-based decision making to understand and assess the risks posed to the transportation system

Key Action
Assessments are conducted using applicant and traveler data to ensure the applicant's eligibility to travel, receive a credential or access, or need for further screening

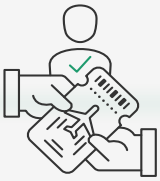


Impact
Technological and functional process improvements enhance speed and accuracy of vetting results for applicants

Identity Verification

Vision
TSA continues to expand its capabilities, including biometrics, to validate and verify an identity and vetting status in real-time (biometric capture only occurs where required or when individuals opt-in)

Key Action
Applicants and travelers' identities are verified each time they use the credential or access



Impact
Expanded biometric capability enables process automation, enhances security effectiveness, and streamlines the passenger and applicant experience

IV. GOALS AND OBJECTIVES

As shown in **Figure 6**, TSA will work to achieve its IDM vision by advancing the overarching goal, four phase-specific goals, and associated objectives.

Figure 6: IDM Overarching Goal and Phase-Specific Goals

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

GOAL 1

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

GOAL 2

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

GOAL 3

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

GOAL 4

Support appropriate **identity verification** activities across TSA

The goals and objectives, while independently important, support each other as they work collectively to advance the overall vision of IDM. Under the overarching goal, there are five cross-cutting strategic drivers that impact and reinforce the phase-specific goals and objectives. In turn, each phase-specific objective aligns with and furthers the cross-cutting strategic drivers. **Figure 7** maps the phase-specific objectives to the cross-cutting strategic drivers to demonstrate their alignment across the IDM strategy. Key topics are introduced in the overarching goal, with further phase-specific details, examples, and caveats provided in each of the phase chapters. This cohesive approach prioritizes the guiding principles of: risk management, person centric, privacy, and resource optimization while upholding privacy and security standards (see Section II: Guiding Principles) .

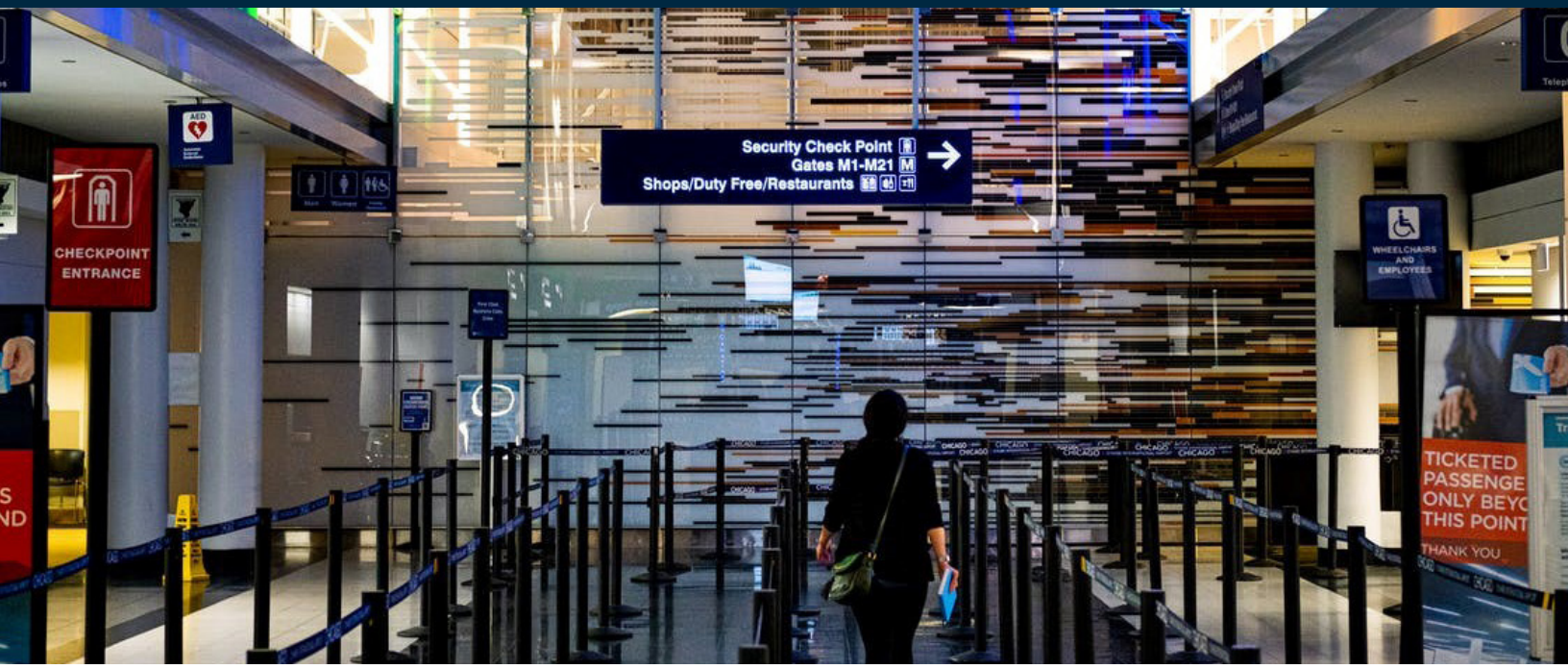
Figure 7: Phase-Specific Goals Aligned to Cross-Cutting Strategic Drivers

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

OBJECTIVE		1	2	3	4	5
Goal 1: Enhance the credential holder and passenger experience during enrollment and travel reservation						
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						
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						
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						
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		✓		✓	✓

OVERARCHING GOAL:



The cohesive future state of IDM works to improve TSA's confidence that an individual accessing the transportation infrastructure is granted the appropriate level of access at the right time. The biographic and biometric information provided by travelers and credentialed populations is used to evaluate and verify an individual's eligibility to safely travel or access secure spaces or information. TSA will continue to monitor and plan for future threat landscapes and mitigation strategies across the transportation enterprise. Building on existing capabilities, TSA will apply innovative functional and technical solutions, including automation, system connectivity, and evaluations of existing and available data. The following cross-cutting strategic drivers explain efforts TSA is making to evolve an efficient, safe, and secure experience for the traveling public and credentialed populations.

Strategic Driver 1
Enhance Standards and the Credential or Access-Based Risk Management Framework

TSA will continue to evolve its risk framework and identity proofing standards to support the dynamic future needs of passenger and credentialed worker populations. TSA will continue to review and update IDM programming for populations tailored to the level of risk undertaken when granting access or provisioning a credential or access to an individual. Updating standards around this risk framework will enable TSA to have a clearer discernment on levels of acceptable risk in various situations, which can enable swift and founded responses to new situations, such as trends around digital forms of identification and access control beyond identity verification. In reviewing its risk management framework, TSA will continue to align and communicate clear and consistent requirements across vendors and systems to support implementation of credential or access-based risk management frameworks.

Strategic Driver 2
Improve Data Sharing Across Systems

TSA will identify opportunities to expand and improve internal and external technical system linkages and potential consolidations, where appropriate, to support operational coordination. In exploring additional linking of data and systems, TSA will work with relevant stakeholders to continue improving the use of real-time identity vetting and verification to determine eligibility and access. Where TSA has already developed robust system connectivity solutions with its partners, these will be evaluated as a part of an effort to develop new standards and scale existing successes. In evaluating new system linkages, TSA will seek information technology security compliance and systems integration, policy compliance and enforcement, and appropriate policy and process changes.

Strategic Driver 3
Evaluate Data Quality and Existing and Available Data Sources

TSA will continue to evaluate the use and value of existing and available data in determining and maintaining a trusted identity and credential or access. TSA will explore biographic and biometric data approaches, including emerging digital identity, to stay ahead of potential threats to transportation spaces and information. Explorations of data usage will inform TSA's ongoing efforts to modernize its technical architecture to support the future needs and data inputs of IDM. This framework will provide innovative and timely improvements to the customer experience while maintaining civil liberties and adhering to governing privacy laws and regulations.

Strategic Driver 4
Improve Self-Service Capabilities for Users

TSA seeks to explore the feasibility of self-service capabilities and improve the passenger and credentialed worker experience when interacting with its systems. TSA will continue to work to improve user experiences through testing solutions that increase the level of self-service and front-end tools available when exploring biometric identity verification solutions. Self-service capabilities enable the user to have more ownership in providing and maintaining their biometric and biographic information. Improvements for credentialed populations could include functionalities to facilitate providing and updating information online (such as address, phone number) and during in-person enrollment or post-enrollment. Providing users more autonomy to update their information will allow TSA to shift resources to address more complex needs. In planning and development, TSA will ensure system and user information security to protect the privacy of credentialed populations and passengers.

Strategic Driver 5
Expand Collaboration Efforts Across U.S. Government and Industry

TSA will deepen relationships across the government, including at the federal and state levels, and with industry partners in the IDM ecosystem to develop collaborative, interoperable, innovative, and timely solutions. TSA will continue to improve the passenger experience by convening and effectively engaging technical and functional subject matter experts across IDM spaces. Collaboration can take shape in many forms, including industry engagement to solicit innovative solutions, topic-specific interagency working groups, and joint pilots across the government (for example, Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Office of Biometric Identity Management (OBIM)) and industry to coordinate IDM efforts for improved user experience and safety and security across the transportation enterprise.

1

ENHANCE THE CREDENTIAL HOLDER AND PASSENGER EXPERIENCE DURING **ENROLLMENT AND TRAVEL RESERVATION**

TSA will continue to improve the passenger and applicant experiences when they provide biometric and biographic data. TSA must collect traveler or applicant information by federal law to keep the Nation's transportation system secure. Effective enrollment of credentialed populations, passengers, and TSA PreCheck® trusted travelers enables security and accuracy throughout the IDM lifecycle. The following phase-specific objectives outline TSA's approach to advancing user experience and the safety and security of the Nation's transportation systems in the enrollment and reservation phase of IDM.

Objective 1.1
Assess and Streamline Data Inputs and Procedures for Interoperability

TSA will explore further standardization and expansion of data inputs across all applicant enrollment and passenger flight reservation platforms and systems to strengthen its confidence in data inputs and data fidelity. TSA will continue to refine data standards and establish firm criteria around the types of data and quality that is accepted to improve confidence in vetting decisions and decrease the amount of redress cases, providing for a more seamless experience for applicants and passengers. Using data-driven risk analyses, TSA will continue to assess the requirements needed to verify an identity to prevent the entry of incorrect information, reduce the number of government and applicant/traveler interactions to correct or add data, and increase TSA's understanding of the applicant or traveler's identity. TSA will continue collaboration with vendors and industry partners (such as airlines, airports, and associations) to develop requirements and pursue this standardization, where appropriate, in alignment with its authorities and regulatory requirements, while prioritizing the safeguarding of information through robust information security procedures.

Objective 1.2
Improve the Accessibility and Convenience of Enrollment/ Reservation

TSA will explore opportunities to work with vendors and shift the way applicants interact with TSA systems and provide data, including assessing the feasibility of implementing new or expanded enrollment platforms (for example, TSA PreCheck). Exploring new enrollment options, such as additional remote channels, provides the opportunity to enhance the user experience. Exploring remote and mobile features of enrollment may offer a more seamless experience for some populations and passengers when interacting with TSA programs. TSA will work with vendors and industry partners to identify and evaluate solutions that provide enhanced enrollment options, primarily for trusted traveler populations initially, that minimize and streamline applicant interactions with TSA. While exploring options, TSA will consider the applicability of mobile and remote enrollment features for various populations and the cost-effectiveness of solutions and data integrity.

Objective 1.3
Explore Partnerships with Industry to Improve the Passenger Experience

TSA will expand and maintain partnerships with industry to identify efficient and effective solutions to enroll passengers and support seamless experiences at check-in and security checkpoints. Partnering with industry will foster development of innovative and scalable concepts to increase data fidelity in enrollment to minimize the need for passengers to resubmit information. When developing new solutions, TSA and its partners will work to ensure clear public and private sector requirements, roles, and responsibilities.

2

CONTINUE TO EXPAND AND EVOLVE STANDARDS FOR **IDENTITY PROOFING** TO SUPPORT FUTURE VETTING AND VERIFICATION ACTIVITIES

TSA is working towards building a real-time picture of who a credential worker or passenger is, as well as confidently asserting that all individuals receiving access have a verified and/or trusted identity at the time of use. Identity proofing, in both the physical and logical contexts, means to confirm people are who they present themselves as and that they have provided accurate biographic and biometric information based on identity assurance best practices. As trends emerge, including mobile and digital identity, TSA will incorporate them into its dynamic strategy while maintaining the rigorous identity proofing necessary to enable confidence in the entire IDM process. These objectives aim to mitigate risk posed by a fraudulent identity and strengthen confidence in trusted identities.

Objective 2.1
Expand Credential or Access-Based Identity Proofing Standards

TSA will continue to evaluate and develop consistent identity proofing standards across programs. TSA looks to refine standards based on the level of risk associated with granting an individual access to transportation systems and information. TSA will continue to leverage standards developed by the National Institute of Standards and Technology (NIST) and other reputable organizations to inform the development of equitable and objective standards. These standards will continue to provide clear guidance on acceptability and applicability of identity documents and information across a variety of touchpoints for credentialed populations and passengers beyond the verification of an identity. These identity proofing standards will facilitate industry's ability to develop new biometric capture or digital identity products and solutions that meet TSA's future goals. This will require ongoing collaboration and communication with industry partners and continued identification of leading practices and application of technologies in the proofing phase.

Objective 2.2
Expand Connectivity and Partnerships to Validate Enrollment/Reservation Data

TSA will build upon existing partnerships and initiate new relationships across government and industry to validate data directly with the original data source, thus strengthening data fidelity and continuing to enable identity assurance. Additional linkages and access to data sources can support further proofing of submitted documents and information in the enrollment or reservation process, meaning more confidence that people are who they say they are. This confidence enables expedited TSA decision making when granting an individual access to secure areas. Improved data fidelity also reduces the burden on passengers by minimizing travel delays or the need to clarify information in the vetting and identity verification phases. Although this objective focuses on credential and TSA PreCheck applicants, the efforts could be scaled further to include additional connectivity in general passenger identity proofing through opt-in practices, while adhering to information sharing laws governing TSA's actions.

Objective 2.3
Explore Automation to Improve Data Collection

TSA will employ innovative technologies to bolster data fidelity and expedite proofing procedures for a faster and more accurate experience. This expands on existing efforts to validate data, either when the applicant uploads a document or when TSA operators review enrollments or reservations.

Automating the population and validation of data fields into an application (for example, using document scanning and automated field inputs) lessens the burden on passengers and applicants and would reduce potential for manual entry errors. This improves data integrity in all subsequent phases of the IDM lifecycle. TSA will need to consider cost and interoperability factors when evaluating potential solutions.

3

CONTINUE TO EVOLVE THE **VETTING** CAPABILITY IN RESPONSE TO NEW THREATS, POLICIES, AND TECHNOLOGIES

TSA will continue to use identified leading practices and evidence-based decision making, as well as evaluate innovative ideas and emerging vetting trends, to assess the risks posed to the transportation system by the individuals accessing it. A person's identity remains at the core of effective vetting, with vetting connecting enrollment and identity proofing to verification. At TSA, vetting is defined as the process by which the data provided by credentialed populations, TSA PreCheck applicants, and passengers are processed through the appropriate checks to determine whether a credential or access can be granted based on established authorities and guidelines governing TSA's operations. The objectives in the following section aim to map the technology, data, and process improvements available to enhance vetting capabilities as threats continue to evolve.

Objective 3.1
Evolve Use of Existing and Available Biometric and Biographic Data

TSA will conduct risk assessments and additional analyses to explore how to evolve the use of existing and available data in its vetting processes. These risk, policy, and viability analyses will directly inform future planning on data collection and vetting checks which are run when granting an individual with a credential or access. TSA will explore and maintain awareness of the data trends of the future, including digital identity, to understand the most important and useful data to determine risk undertaken when provisioning a credential, access, or travel authorization. TSA recognizes its important role in safeguarding the personal information and data that individuals provide to TSA in enrollment and reservation processes and will continue to adhere to laws on safeguarding data and data use. For more information on biometric information TSA collects and how it uses this information, please reference the Biometrics Roadmap.

Objective 3.2
Apply Credential or Access-Based Risk Framework to Vetting Practices

TSA will continue to make vetting determinations based on the credential or access requested, informed by a risk framework tailored to the risk level of varying access points to maintain confidence in the integrity of transportation spaces. This application works to enable the future vision of IDM to cohesively use the lifecycle phases to grant access to the right individuals at the right times at the right access points (for example, cargo loading areas have different risks and vetting needs from expedited screening lanes). TSA will evaluate vetting checks, such as terrorist watch-lists, to inform alignment with the credential or access-based risk frameworks across the IDM lifecycle. TSA's evaluation of the risk framework's application will be performed in alignment with its existing authorities and policies, and with privacy and civil rights and liberties at the core of any changes.

Objective 3.3
Explore Automation to Improve Vetting Processes

TSA will explore innovative technical and functional improvements to vetting processes, procedures, and systems, such as automation to provide more real-time vetting determinations. This objective builds on continued efforts to modernize vetting based on the best-suited tools and resources available to enable real-time use of the vetting determinations at passenger or credentialed worker access points. TSA will explore options across the government and industry for adapting technical solutions to enhance efficiency of systems and infrastructure to reduce manual, repetitive tasks and increase the application of unique human skills, in alignment with the risk management framework. TSA will employ subject matter experts across government and industry when creating timely improvements for TSA's vetting capability. TSA will consider cost-effectiveness, interoperability, and the impact on vetting staff of automation solutions when identifying implementation options.

4

SUPPORT APPROPRIATE **IDENTITY VERIFICATION** ACTIVITIES ACROSS TSA

TSA seeks to keep improving its ability to validate and verify identity and vetting status in real-time when the credential or access is used. As articulated in the Biometrics Roadmap, TSA is moving toward biometric identity verification, where applicable by statute and regulations, for passenger populations and, in the longer term, for credentialed worker populations.

Objective 4.1
Continue Developing Identity Verification Solutions for Passenger Populations

TSA will expand on its efforts to provide enhanced identity verification solutions for passenger populations at the checkpoint, more confidently confirming a passenger's flight and vetting status and identity, while creating a more modern and expedited travel experience. This objective builds on plans already in the implementation phase and in response to shifts in global travel patterns and expectations. TSA looks to expand the number of airports that use Credential Authentication Technology (CAT) to verify and validate a person's identity and flight status. It will develop, test, and refine ways to reduce touch interactions with Transportation Security Officers (TSO) through self-service as much as possible. In executing this objective, TSA will prioritize integration with existing systems, including screening systems to support potential downstream activities like risk-based screening, impacts on TSOs and their operating procedures, as well as passenger expectations at the checkpoint.

Objective 4.2
Explore Modernizing Verification Solutions for Non-Passenger Populations

TSA will apply lessons learned from implementing CAT at airport checkpoints to non-passenger populations such as known crew members, aviation workers, and law enforcement/federal air marshals. TSA will build on the passenger solution architecture to bring benefits that travelers experience to credentialed populations. As TSA aims to prioritize security over efficiency, when applicable it will explore solutions to reduce specialization where security gaps emerge or exist because of specialized processes. For those populations already providing biometrics and receiving security threat assessments, TSA will look to leverage this information where appropriate to expedite verification for those whose employment falls beyond the airport checkpoint. TSA recognizes the unique needs of non-passenger populations and as such, it will prioritize coordination with relevant industry and government parties. It will also look to incorporate flexibility when designing future solutions and to scale capabilities and technologies already successfully implemented at airports before considering net-new solutions.

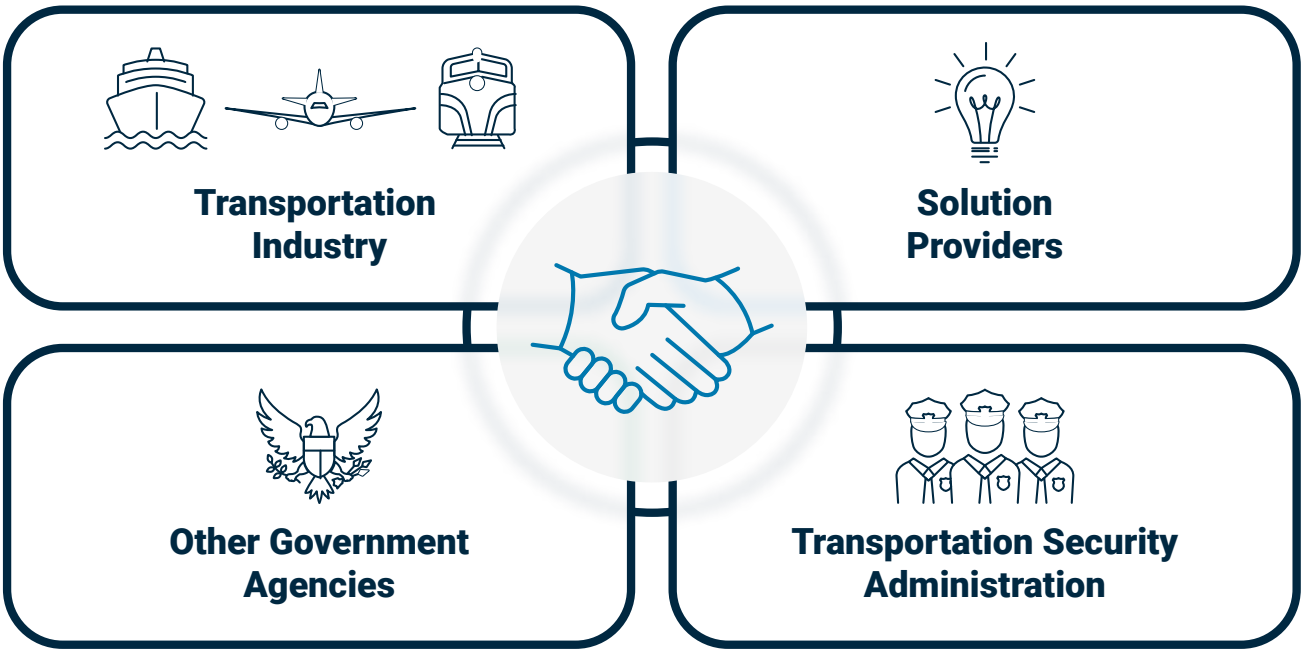
Objective 4.3

Engage Industry and Interagency Partners to Enable Biometric and Digital Identity Solutions

TSA will engage industry and interagency partners to expand the use and integration of digital identity solutions in its transportation arenas to mirror customer expectations (for example, digitization of key services and experiences) in their travel experience. Three key partnerships TSA will prioritize when exploring this area are its work with (1) external partners to identify opportunities to integrate their digital identity solutions for customers into the infrastructure of airports and TSA systems, (2) DHS partners such as the OBIM, CBP, and DHS Science and Technology Directorate to explore leading practices and additional data sources and linkages, where appropriate, and (3) the U.S. Government on REAL ID and digital ID responses and products to ensure alignment and seamless use of digital identity products by citizens across all government interactions. In pursuing these goals, TSA will review state and federal biometric laws and limitations and adhere to information security and privacy requirements to protect individuals' information.

V. MOVING FORWARD

This Roadmap will guide future efforts, studies, pilots, and program implementation across TSA's IDM ecosystem. Following its publication, TSA will develop subsequent activities, engagement strategies, and work plans in consultation with government and industry stakeholders. The approach will require continued collaboration between TSA and its partners to maintain and scale existing capabilities and iteratively develop new capabilities across populations in accordance with applicable laws, authorities, civil rights and liberties, and privacy protections. Just as each phase of IDM builds on one another, so does the collaborative efforts of all partners to make the future vision of IDM a reality.



VI. Appendices

APPENDIX A: Acronyms & Terms

Acronym	Term
CAT	Credential Authentication Technology
CBP	Customs and Border Protection
DHS	Department of Homeland Security
IDM	Identity Management
OBIM	Office of Biometric Identity Management
TSA	Transportation Security Administration
TSO	Transportation Security Officer

Term	Definition
Credential or access	The intended license, privilege, or status granted as a result of approved checks. It remains valid until the credential/access expires and/or is revoked.
Enrollment	Collection of biographic and biometric information through in-person and virtual platforms, where applicable.
Identity proofing	Validation of provided biographic and biometric information in accordance with TSA's standards (derived from NIST 800-63A) by confirming that provided information matches with a trusted source.
Identity management	The holistic process of enabling the right person to have the right access or credential based on their biographic and biometric information.
Identity verification	Match a person's physical or digital identification/biometrics against the vetted information to verify a person's identity at credential or access use (e.g., access to secure area, differentiated level of physical screening).
Issuance/credentialing	Entire process (from application through issuance, use, and expiration or potential revocation of the issued credential) of determining a person's suitability for a particular credential, access, or status and assigning a token that enables use of the credential, access, or status.
Population	A managed group of individuals applying for similar credentials or accesses within the transportation security enterprise.
Provisioning	Assigning a token that enables use of the credential, access, or status.
Reservation	Collection of biographic information, or biometric information where applicable, from passengers at the time of booking travel.
Vetting	Acquiring the appropriate data and running the appropriate checks to determine if the credential or access can be granted.
Industry	Including but not limited to Air Carriers, Air-Carrier Representation, All-Cargo Air Transportation, Labor Organizations representing Air Carrier Employees and TSOs, Airport Operations.

APPENDIX B: TSA's Commitment to Privacy

TSA is committed to protecting passenger privacy and ensuring the public's trust as it seeks to improve the passenger experience through its improvements to IDM capabilities. TSA regularly engages with TSA and DHS's Privacy Offices and Offices of Civil Rights and Civil Liberties to evaluate the potential privacy impacts of enrollment, identity proofing, vetting, and identity verification. These engagements help TSA develop appropriate procedures to mitigate privacy impacts, and ensure that our vetting and identity verification solutions are deployed in a manner that protects travelers' civil rights and civil liberties.

TSA will continue to incorporate privacy considerations into each action we take in pursuit of enhancing the Identity Management Portfolio. Solutions will be designed to secure data at rest and in-transit to protect both passengers and system integrity across the data lifecycle.

TSA will comply with section 208 of the *E-Government Act of 2002*, section 222 of the *Homeland Security Act of 2002*, and DHS's privacy compliance process. As such, it will conduct appropriate privacy threshold analyses, privacy impact assessments, and system of records notices when considering the use of new or enhanced solutions with potential privacy impacts. TSA will also comply with applicable TSA, DHS, and Office of Management and Budget policies and authorities governing the handling of personally identifying information.

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

APPENDIX C: Strategic Alignment

Organization	Document Name
DHS	Department of Homeland Security Biometric Framework 2015-2025 Department of Homeland Security Strategic Plan 2020-2024
TSA	TSA Strategy 2018-2026 Administrator's Intent 2020 Biometrics Roadmap 2018 TSA Strategic Five-Year Technology Investment Plan (Biennial Refresh) 2017
CBP	CBP Biometrics Strategy 2021-2026
OBIM	TSA - OBIM Biometrics Strategy and Multi-Year Integrated Roadmap 2020 Office of Biometric Identity Management Strategic Plan 2019-2023 and Implementation Approach

APPENDIX D: Stakeholders Consulted

Stakeholder Name	Stakeholder Alignment
Department of Homeland Security (DHS) Science & Technology (S&T) Directorate	Government
DHS Office of Biometric Identity Management (OBIM)	Government
TSA Internal Stakeholders (Various)	Government
U.S. Customs and Border Protection (CBP)	Government
U.S. Citizenship and Immigration Services (USCIS)	Government
International Air Transport Association (IATA)	Industry Association
National Air Carrier Association (NACA)	Industry Association
Regional Airline Association	Industry Association
Airlines for America (A4A)	Industry Association
Airline Service Provider Association (ASPA)	Industry Association
Airport Council International (ACI)	Industry Association
American Association of Airport Executives (AAAE)	Industry Association
National Business Aviation Association (NBAA)	Industry Association
Customized Logistics and Delivery Association (CLDA)	Industry Association
Airforwarders Association	Industry Association
NATA Compliance Services	Industry Association
General Aviation Manufacturers Association (GAMA)	Industry Association
Aviation Security Advisory Committee (ASAC)	Industry Association
Surface Transportation Security Advisory Committee (STSAC)	Industry Association