Open Architecture Roadmap

July 2023

Version 1

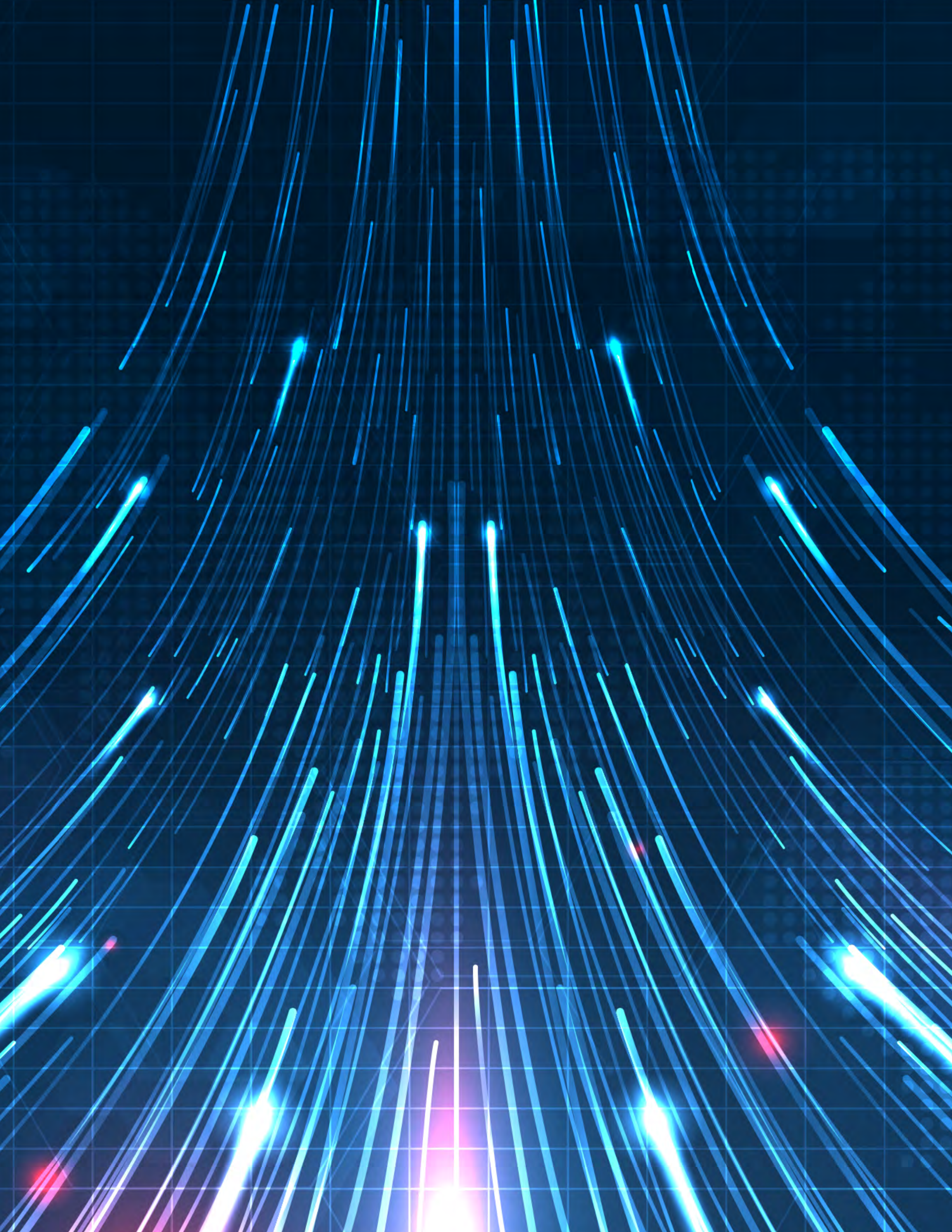


Table of Contents

Table of Figures

scan
DETECT 1000
S-013846
S-057861
S-014689

Administrator's Message

The Transportation Security Administration's (TSA) mission is to protect the Nation's transportation systems to ensure the freedom of movement for people and commerce. To achieve this mission in an evolving threat environment, TSA must prioritize being an agile and flexible organization which can rapidly field innovative screening solutions capable of improving TSA's security posture. It is essential we do this while maintaining a commitment to our frontline workforce and the traveling public.

To accomplish this, we must implement innovative screening solutions in a manner that supports the Transportation Security Officer in conducting critical screening functions, improves screening efficiency and enhances customer experience. Using an open architecture design approach will allow TSA to improve its security posture, support its frontline workforce, and promote an enhanced customer experience.

The Open Architecture design approach is founded on the concepts of having equipment components, such as software and hardware, that are standards-based and interoperable. This affords TSA the ability to use strategic industry and international partnerships that allow for the adoption of increasingly interconnected technologies while employing advanced cybersecurity capabilities. Open Architecture expands our engagement with innovative partners, such as small businesses and academic institutions, while maintaining the relationships we have with industry vendors.

This roadmap will serve as a foundation that builds on the vision outlined in the TSA Strategy (2018–2026), the Administrator's Intent 3.0, TSA Innovation Doctrine, and TSA's Capability Roadmaps to holistically guide TSA's Open Architecture goals and objectives.

I thank everyone at TSA and our interagency, industry, and international partners who contributed to the development of this roadmap. As Open Architecture concepts mature, continuing to work together will allow us to realize this vision and improve security effectiveness and customer experience, support TSA's frontline workforce, and expand industry and international engagement. This is a global aviation security priority.

David P Pekoske

David P. Pekoske
Administrator

Introduction

TSA's current security screening system is highly complex with limited data or interface standardization. Lack of standardization presents barriers to TSA achieving the desired security posture and hinders its ability to rapidly deploy innovative screening solutions to the field to respond to the evolving threat environment. It also increases the burden on our frontline officers who must perform their critical screening functions with cumbersome procedures, complex training, and varying user interfaces.

Open Architecture (OA) is a design approach in which equipment components, such as software and hardware, are standards-based and interoperable to allow a wide range of industry partners to create improved subcomponents (like new detection algorithms, user interfaces, or reporting systems). Using this approach will allow TSA to establish a superior transportation security System of Systems (SoS) that interact with each other and provide a unique capability that cannot be accomplished independently.

TSA has a history in supporting OA concepts dating back to 2010. TSA worked in partnership with industry to establish the first security image data standard. TSA has subsequently continued to support the maturing of this standard through three formal updates. Over the past five years, TSA has accelerated its efforts related to OA and is well positioned to take the next steps to operationalize mature OA concepts while applying lessons learned from other government, industry and stakeholder organization efforts and TSA's innovation experience.

Applying an OA approach benefits TSA by:

- Improving the performance of the security mission.
- Supporting our frontline workforce.
- Improving the customer experience.
- Enhancing engagement with the security industry.

The successful implementation of this approach will require coordination across a wide range of partners like government agencies, stakeholder organizations, industry and international partners, national labs, academia, airlines and airports. TSA further aims to use the best practices of the Department of Defense (DOD) Modular Open Systems Approach (MOSA) to achieve the goals and objectives outlined in this roadmap.

Purpose and Scope

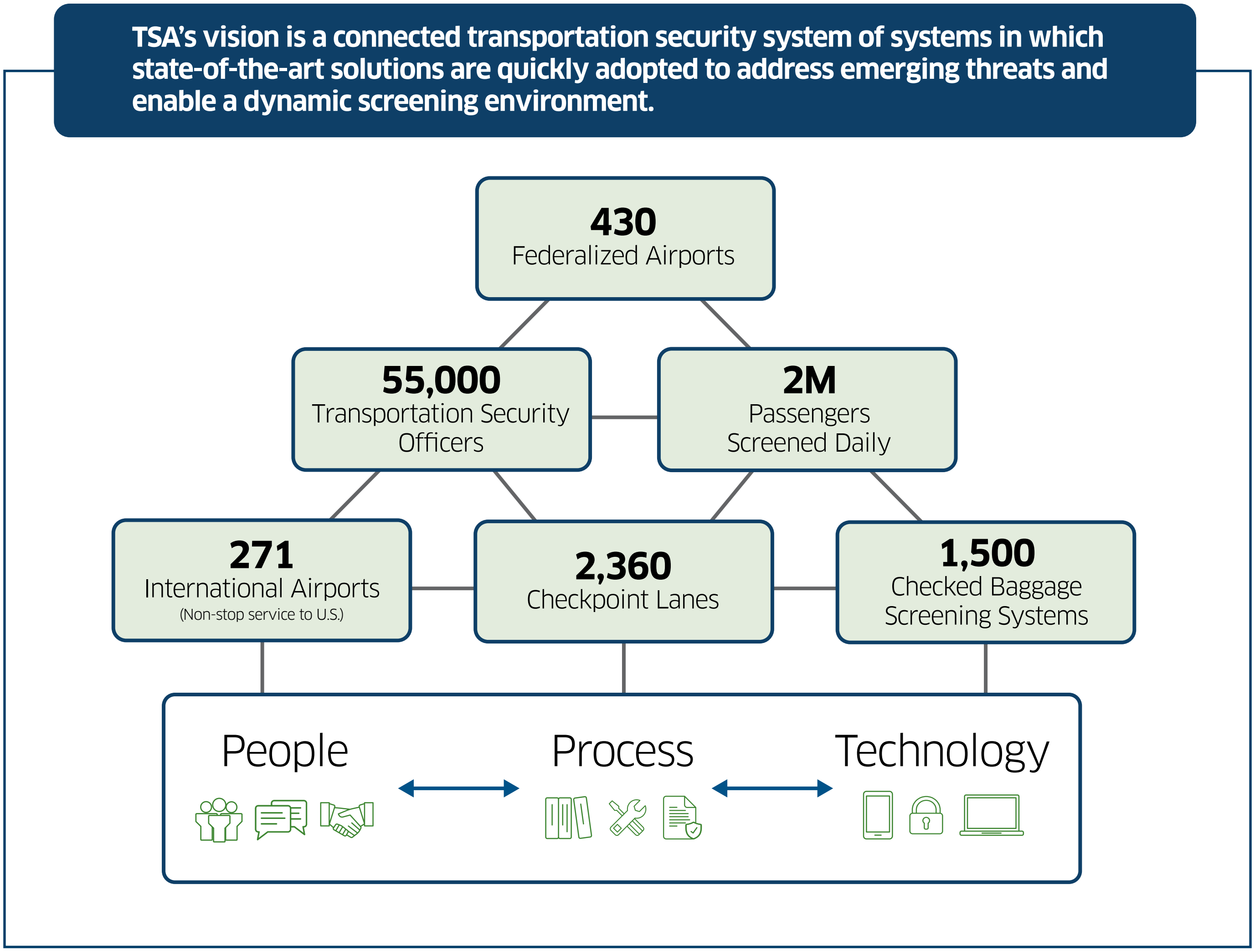
TSA is challenged with the need to establish an SoS for 55,000 officers who screen over 2 million passengers, on average, per day at over 430 federalized airports with nearly 1,500 checked baggage systems and 680 checkpoints with 2,360 lanes. The current solution limits our capability to use various vendor implementations, puts significant burden on our frontline workforce who must contend with the variation across configurations, impacts our ability to respond to threats, and limits integration of new technology. It is imperative that the SoS be standards-based to support interoperability and allow for partnerships across the security industry while providing the frontline workforce with the tools they need to perform the mission.

This roadmap serves as a foundation for providing TSA's vision, goals, and objectives to establish a connected transportation security SoS, using OA guiding principles. It will guide TSA's OA activities and identify short-term (within 3 years) and long-term (more than 3 years) needs to sustain success. The roadmap will evolve and create more detailed artifacts (like standards, guidelines, and requirements) as TSA partners with industry and stakeholder organizations to implement OA goals and objectives.

Vision

TSA's vision is a connected transportation security SoS in which state-of-the-art solutions are quickly adopted to address emerging threats and enables a dynamic screening environment. This vision outlines our commitment to our most important asset, the dedicated frontline officers, securing the transportation system. Our vision seeks to provide the best tools to conduct mission critical screening operations while simplifying processes and procedures. Figure 1 illustrates that this vision encompasses the combination of people, processes, and technologies across capability areas like identity management, accessible property screening, on-person screening, checked baggage screening, and alarm resolution.

Figure 1. SoS Vision Across TSA Mission Space



TSA's vision is a connected transportation security system of systems in which state-of-the-art solutions are quickly adopted to address emerging threats and enable a dynamic screening environment.

430
Federalized Airports
55,000
Transportation Security Officers
2M
Passengers Screened Daily
271
International Airports
(Non-stop service to U.S.)
2,360
Checkpoint Lanes
1,500
Checked Baggage Screening Systems
People
Process
Technology

Strategic Drivers

The following strategic drivers are the catalysts for defining and pursing the OA goals and objectives.

- **Improve Security Effectiveness and Agility:** TSA must be able to proactively address the threat. This requires the ability to rapidly respond to emerging and evolving threats. An OA approach allows us to introduce improved algorithms, user interfaces, or other potential solutions to the screening environment faster and with greater flexibility (for example, plug and play). By leveraging OA principles, we increase the ability to deliver enhanced processes and technology capabilities to the field in a timely manner. This supports establishing a future-ready transportation security SoS that is more effective and builds Transportation Security Officer (TSO) trust in the systems' performance.

- **Support the Frontline Workforce:** The variety of transportation security equipment (TSE) in use has significantly complicated the TSA screening mission. This complexity is evident by the various user interfaces, training, and procedures required to utilize the different types of equipment. The collective transportation security system of people, processes, and technology must be taken into account to ensure that processes and technology are optimized for the 55,000 dedicated TSOs performing the mission. This means focusing on simplifying technology and processes, standardizing user interfaces, and rapidly responding to user needs.

- **Improve Operational Efficiency:** TSA must optimize the use of the TSE to increase overall capacity of the transportation security SoS. As passenger volumes increase, the space needed to conduct current screening approaches will not keep pace. Therefore, TSA must use OA principles to find solutions to reduce false alarms, improve TSO performance through simplifying the screening process, and establish capabilities for improving overall TSE use (for example, remote screening).

- **Improve the Customer Experience:** TSA needs to support efficiencies with tailored screening approaches, risk-based methodologies, reduced divestiture of items, and a more streamlined experience like the One-Stop Security concepts that will potentially alleviate the need to rescreen passengers and luggage when traveling abroad. Applying risk-based methodologies will provide a tailored screening approach for passengers, resulting in an improved experience. As TSA implements innovative industry solutions, we expect passengers will encounter fewer false alarms on their person and baggage. As a result, fewer pat-downs and bag searches will be needed, further improving the customer experience.

- **Expand Industry and International Engagement:** To address the security mission, it is important to have a diverse marketplace. OA is key to supporting innovation from the entire community and providing a pathway to breakthrough capabilities because it positions TSA to implement multiple contract awards targeting specific components of the SoS. This multiple contract award approach reduces the risks and up-front investment (that is, lowers the barrier to entry) associated with delivering a complete solution for a single contract award. As a result, industry partners can more easily participate within different segments of the transportation security market, based on their desired business model. In working with industry partners, TSA acknowledges the importance of ensuring usability in other mission spaces (like customs and prisons) and protection of intellectual property. TSA aims to support broad use of OA solutions and in ensuring all industry partners – like Original Equipment Manufacturers and third-party developers – have their intellectual property protected. Additionally, because OA is a global aviation security priority, TSA is focused on collaborating with international and government partners to improve aviation security worldwide through shared development activities and joint capability implementation.

- **Improve Cybersecurity:** Cybersecurity requires rigorous and ongoing evaluation of risk and threats, definition of requirements, compliance with appropriate standards and assessments. To fully implement capabilities in an integrated, networked transportation security environment, TSA must improve cybersecurity, using approaches such as the Zero-Trust Model, throughout the design, development, and testing processes to include planned lab and field demonstrations.

- **Implement Tailored Acquisitions:** The current acquisition framework largely consists of implementing single unit, mission capable systems, which are self-contained and use vendor proprietary hardware and software. To realize the full benefits of OA, TSA must work within the acquisition framework to tailor acquisition activities and strategies. Tailored acquisitions will enable TSA to develop, test, deploy, and maintain new capabilities rapidly and efficiently using a more modular and vendor-agnostic SoS approach.

- **Improve Data Analytics and Decision-making:** An open, connected transportation security SoS allows for standardized critical data elements and collection of relevant information, which supports effective decision-making in near real time. OA standardization and connections between systems will position TSA to remain agile and flexible in an increasingly data dependent world.

Guiding Principles

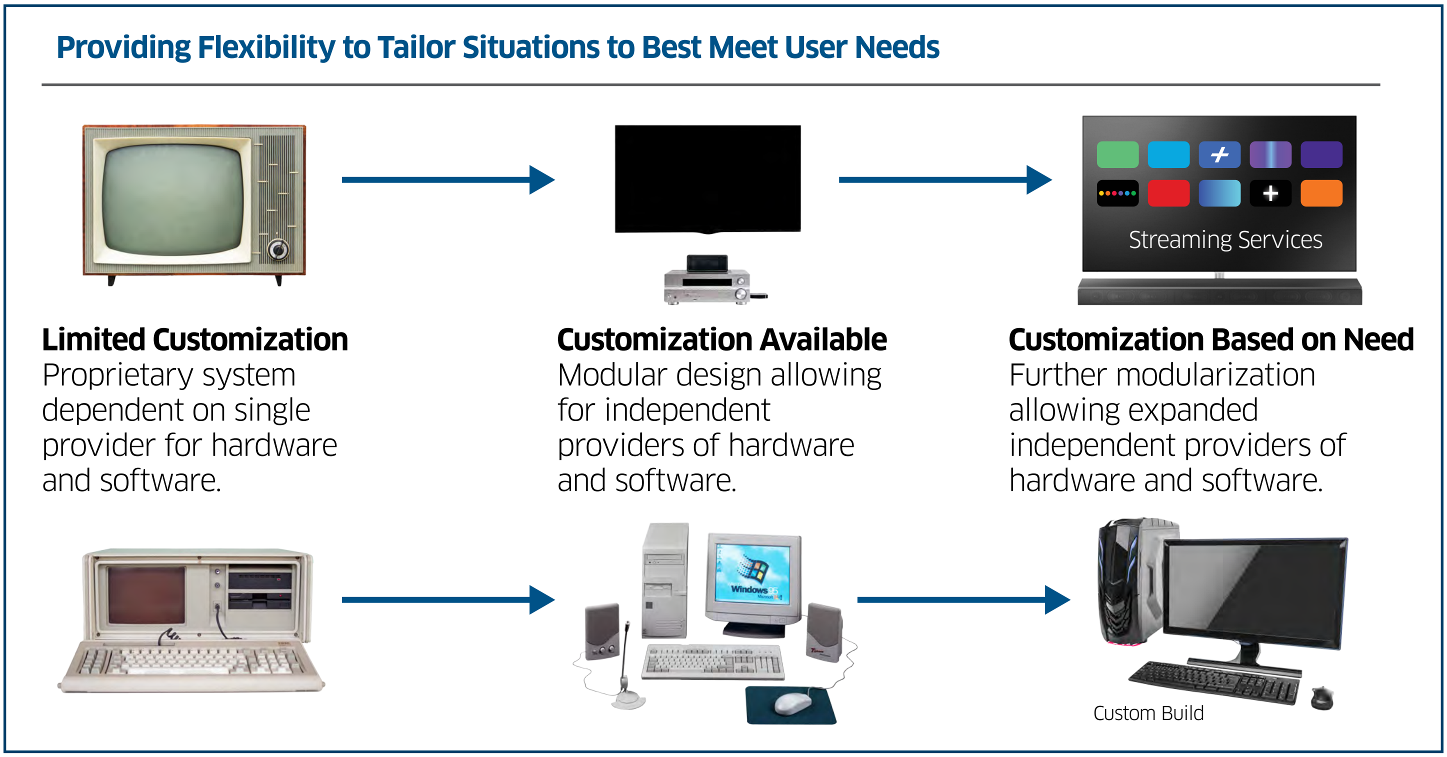
The OA methodology uses the guiding principles of standardization and open data to implement the roadmap's objectives. These principles build on and reinforce common industry concepts and practices.

- **Standardization:** Leverage common and accessible data and interfaces. This requires implementing and maintaining standardized interfaces, data formats, and other appropriate solutions in an intentional and agile approach in partnership with government, industry, and stakeholder organizations.

- **Open Data:** Establish open, high-quality, and comprehensive data sets available to aviation security industry partners.

Figure 2 shows other real-world examples of standardization and open data in the technology field. For example, the first televisions were limited in their ability to rapidly implement new capabilities. As television designs became standardized and more modular, a level of future-proofing provided users a familiar interface while also allowing them to tailor the experience (for example, cable boxes, disc players, software applications). The personal computer is also an example of standardization and open data that allows for a marketplace of various software and peripherals which are compatible with the personal computer.

Figure 2. OA Principles Provide Flexibility to Tailor Solutions to Best Meet User Needs



Providing Flexibility to Tailor Situations to Best Meet User Needs

Limited Customization
Proprietary system dependent on single provider for hardware and software.

Customization Available
Modular design allowing for independent providers of hardware and software.

Customization Based on Need
Further modularization allowing expanded independent providers of hardware and software.

Future State

TSA is committed to an open, connected, responsive, and flexible transportation security SoS. To achieve this future state requires the following:

- **Engagement:** TSA will engage and coordinate across government and with regulators, stakeholder organizations, industry and international partners, national labs, academia, airlines and airports. TSA will establish communication channels at strategic, programmatic, and technical levels. These channels will promote collaboration, continued progress, establishment of joint standards, and new ideas in partnership with stakeholders.

- **Technical Standards and Capabilities:** Success depends on common and accessible data and interface formats. TSA will partner with industry stakeholders to identify appropriate standards for adoption. Standardization will improve TSA's ability to provide consistent training, implement best practices for human factors, share information in real time for backend development and analytical purposes, allow for component level testing, and apply risk-based screening methodologies while optimizing the use of screening solutions. TSA will provide a means to update, maintain, and evolve solutions over time to ensure continued interoperability and an ability to align with industry best practices and innovation. In addition, TSA will be intentional and transparent about adopting standards to promote innovation in the market while avoiding impeding delivery of mission critical capability to the field.

- **Organizational Policy and Procedures:** As TSA begins to take the next steps toward that future state, our current operating models, policies, processes, and resourcing will need to be evaluated to ensure an effective long-term strategy that aligns with internal and external stakeholders. We understand that the strategy, objectives, and goals outlined in this roadmap are not without challenges. TSA will take advantage of OA capabilities to incrementally evolve existing policies and processes in collaboration with our stakeholders to minimize risk and apply lessons learned.

- **Data Sharing:** Technical standards and capabilities allows us to collect data and support rapid development of new algorithms and other solutions. To capitalize on this capability, TSA will establish comprehensive and high-quality screening data sets and improved pathways to share data with approved vendors to develop and test solutions. TSA will partner with government, industry, and stakeholder organizations to define appropriate data collection, annotation, storage, and distribution methodologies. Agreement on these approaches will support data security, industry growth, and cost efficiencies through shared data models.

Goals and Objectives

To minimize risk while enabling continued progress and growth, TSA will take an agile approach to achieve each goal and objective defined in this section. As these goals and objectives cross all of TSA's mission capability areas, we will incrementally introduce solutions into each capability roadmap.

The evolution of capabilities will consider upgrades, enhancements or recapitalization of technologies. Each policy, process, and solution is expected to continually evolve in support of TSA's mission as we work toward an open, connected transportation security SoS. Continued coordination on OA concepts will help promote a unified market for aviation security equipment and reduce variation and complexity for industry in its development of solutions. Figure 3 illustrates TSA's vision and goals for:

- Engagement
- Technical standards and capabilities
- Organizational policies and procedures
- Data sharing

Figure 3. OA Goals

Vision
TSA's vision is a connected transportation security system of systems in which state-of-the-art solutions are quickly adopted to address emerging threats and enable a dynamic screening environment.

Goal 1 Engagement
Implement enhanced coordination and communication with government, industry, and stakeholder organizations at the strategic, programmatic, and technical level to build partnerships in the development of an open, connected transportation security system of systems.

Goal 2 Technical Standards & Capabilities
Establish and adopt open architecture technical standards and capabilities to enable interoperability and a flexible, plug and play screening environment.

Goal 3 Organizational Policy & Procedures
Evaluate policies, processes, products, and organizational needs to support the implementation and management of open and interoperable transportation security system-of-systems solutions.

Goal 4 Data Sharing
Enable rapid solution development to improve emerging threat response and adoption of best-in-class security innovations.

Engagement

Goal 1: Implement enhanced coordination and communication with government, industry, and stakeholder organizations at the strategic, programmatic, and technical level to build partnerships in the development of an open, connected transportation security SoS.

Objective 1.1: Communicate and coordinate strategic and programmatic initiatives with government, industry, and stakeholder organizations and facilitate ongoing engagement.

TSA will continue to outline the vision, goals, and objectives of this roadmap as we learn more through implementation. We expect this roadmap to help mature OA concepts and as it does, it may need to be updated and could support development of more detailed artifacts. TSA will communicate major strategy updates to industry in a consistent voice to ensure effective policy development and interpretation.

TSA will need many combinations of stakeholder solutions to achieve a connected transportation security SoS. Therefore, we will continue to partner with government, industry and stakeholder organizations to promote transparent communication of initiatives as appropriate throughout the development, demonstration, and implementation process. This will help showcase progress, enable adoption of successful solutions, and incorporate lessons learned into the development process.

TSA will also establish a comprehensive field engagement strategy to ensure adopted solutions are successfully implemented. TSA will seek to leverage the experience, capabilities, and authorities, of other government agencies and stakeholder organizations with shared goals. Additionally, TSA will collaborate with industry to achieve a system that considers industry needs while enhancing TSA's ability to carry out its mission.

As an example, One-Stop Security is a partnership with TSA, U.S. Customs and Border Protection (CBP), and several domestic and international partners working towards a security solution alleviating the need to rescreen passengers and luggage when traveling into the United States and abroad. This initiative is balanced with the need to ensure TSA's implementation drives toward a connected transportation security system that meets the needs of over 430 federalized airports in the United States.

Outcome: Establishment of a coalition of stakeholders to successfully mature open and connected SoS concepts.

Objective 1.2: Implement recurring technical forums, working groups, and methodologies to enable collaboration and continuous improvement of OA technical standards and capabilities.

TSA will establish and support technical forums and working groups to provide a platform for government, industry, and stakeholder organizations to collaborate on the adoption and maintenance of approved technical standards and capabilities. An open, connected transportation security SoS is never complete and must continue to evolve over time. Technical forums and working groups allow the subject matter experts from TSA, industry, and stakeholder organizations to partner on both current and future OA solutions while promoting continued innovation in the market. The form of these initiatives may vary depending on the specific component considered.

As a global aviation security priority, TSA engages directly with international partners in pursuit of harmonizing OA solutions. These solutions help provide a unified market for aviation security equipment and reduce variation and complexity for industry in their development of them.

Outcome: Forums consisting of TSA, industry, and stakeholder organizations to discuss, define, and maintain current and future technical standards and capabilities.

Technical Standards and Capabilities

Figure 4 illustrates TSA's plan to conduct continuous development and testing and phase-in capabilities by TSA capability areas.

Figure 4. Adoption of Technical Standards and Capabilities

Adoption of Technical Standards and Capabilities

Continuous development and testing of OA design approach and components

Adoption of technical standards and capabilities phased-in by TSA capability areas

Goal 2: Establish and adopt OA technical standards and capabilities to enable interoperability and a flexible, plug and play screening environment.

Objective 2.1: Adopt common and accessible data format through real-time Digital Imaging and Communications in Security (DICOS).

DICOS was established in 2010 in partnership with the National Electrical Manufacturers Association (NEMA) and is based on the Digital Imaging and Communications in Medicine (DICOM) standard, which provides a successful example of common data implementation across a complex market. It also provides valuable lessons learned for TSA and industry to apply to the security screening domain. The DICOS standard provides a common, accessible data file format to enable the exchange of consistent information for security screening equipment that maintains a high quality image. TSA will implement real-time DICOS for screening solutions to ensure the exchange of consistent information and to improve the ability to share data with industry partners. TSA will collaborate with industry stakeholders to define, develop, and maintain the DICOS standard and supporting solutions.

TSA expects to initially adopt real-time DICOS for accessible property screening solutions (that is, Checkpoint Computed Tomography (CT)) before moving on to additional capability areas as appropriate while applying lessons learned and other applicable industry standards.

Outcome: Common and accessible data to enable rapid solution development and an ability to transmit data across TSE in live screening operations.

Objective 2.2: Adopt common and accessible interface format through Open Platform Software Library (OPSL).

OPSL is a common, accessible set of application programming interfaces. These interfaces standardize how software can interact with each other to enable interoperability between screening solutions. TSA will implement OPSL to enable systems and system components to share and move data consistently across the transportation security SoS. OPSL will enable an interoperable transportation security SoS in which TSA and industry partners can more easily incorporate new solutions into the screening environment.

As TSA adopts OPSL, it will transition to a user-driven software project to ensure end-user usability, solution transparency with approved parties, and improved speed and quality in the development, testing, and maintenance of OPSL. TSA views a future where OPSL is maintained and matured through a collaborative effort with all of industry and TSA has a level of governance to ensure releases are available to all of industry. In this model, TSA facilitates:

- prioritization and approval of features and updates.
- coding best practices and quality.
- cybersecurity standards.

Industry partners will:

- have access to the source code.
- propose and develop improvements at their pace.
- implement improvements with permission and in coordination with TSA.

The user-driven OPSL model enables TSA to use open-source software development as well as industry best practices and talent to continuously develop, test, and maintain OPSL for the long-term. Additionally, a user-driven model provides industry with maximum code transparency to adapt their capabilities to be OA compliant. It also improves code at a tempo consistent with TSA mission and industry needs.

TSA expects to initially adopt OPSL in a limited capacity for accessible property screening solutions while transitioning to a user-driven model. As TSA implements and transitions OPSL, TSA expects to improve and mature OPSL capabilities in partnership with industry stakeholders before applying lessons learned to other capability areas.

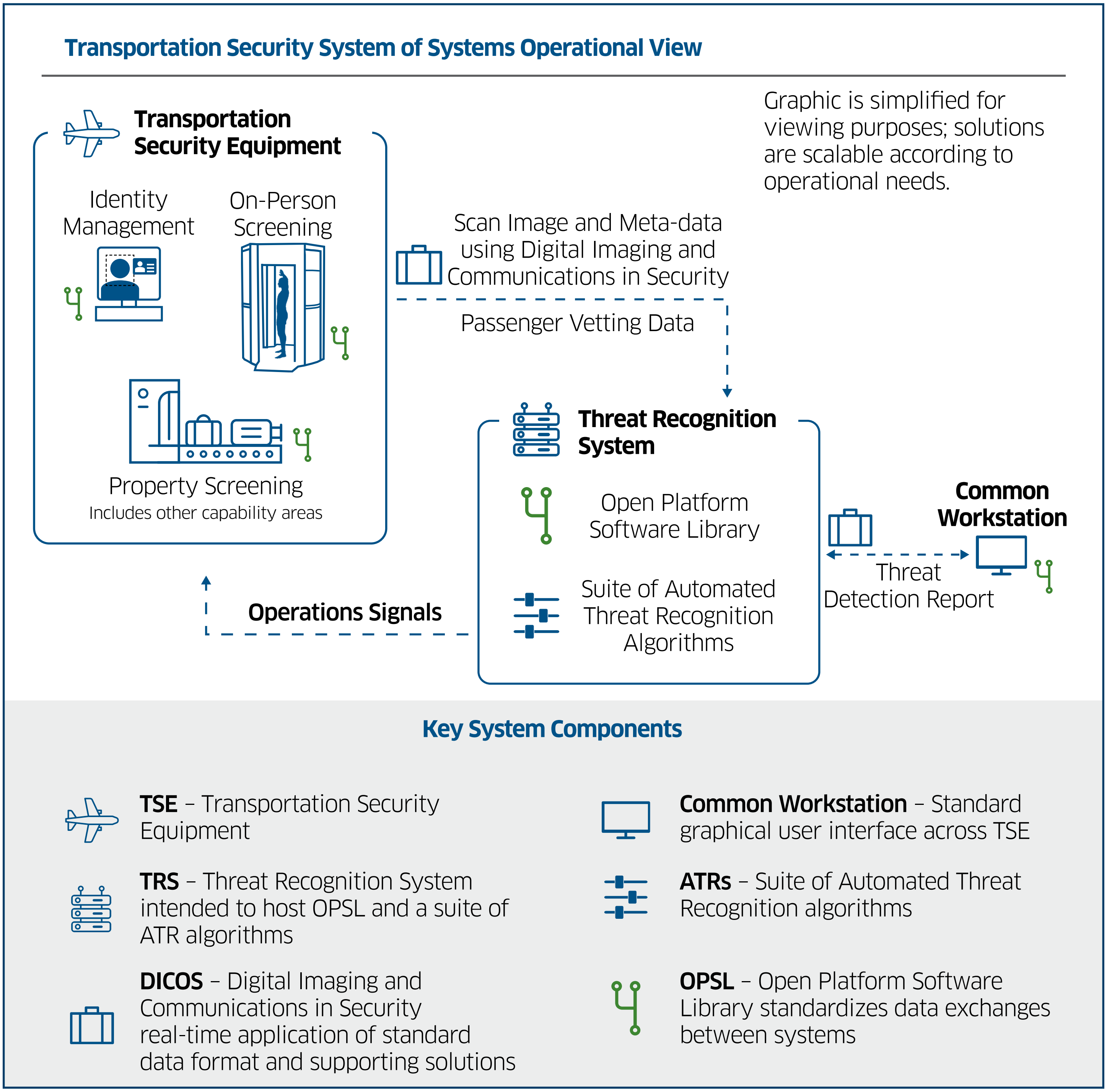
Outcome: Common and accessible interfaces and communications to enable the implementation of an open transportation security SoS.

Objective 2.3: Demonstrate a scalable and common computing platform to provide an open transportation security SoS solution.

While DICOS and OPSL have been successfully tested with multiple vendors, there is still a need to demonstrate operational performance and functionality of a complete solution using DICOS and OPSL.

Figure shows TSA's concept of the Threat Recognition System (TRS) which combines the computing hardware, DICOS, and OPSL to provide a platform for integrating screening equipment, establishing a scalable computing approach to leverage algorithms from industry partners, and allowing for a common workstation. The TRS approach provides a common operational solution to minimize cybersecurity vulnerabilities and improves the ability to mitigate emerging cyber threats. TSA has conducted multiple small-scale demonstrations to mature TRS and evaluate the performance requirements needed to provide an operationally viable and cyber secure solution.

Figure 5. Transportation Security System of Systems Operational View



Transportation Security System of Systems Operational View

Graphic is simplified for viewing purposes; solutions are scalable according to operational needs.

Transportation Security Equipment
Identity Management
On-Person Screening
Property Screening
Includes other capability areas
Scan Image and Meta-data using Digital Imaging and Communications in Security
Passenger Vetting Data
Threat Recognition System
Open Platform Software Library
Suite of Automated Threat Recognition Algorithms
Operations Signals
Common Workstation
Threat Detection Report

Key System Components

TSE – Transportation Security Equipment

TRS – Threat Recognition System intended to host OPSL and a suite of ATR algorithms

DICOS – Digital Imaging and Communications in Security real-time application of standard data format and supporting solutions

Common Workstation – Standard graphical user interface across TSE

ATRs – Suite of Automated Threat Recognition algorithms

OPSL – Open Platform Software Library standardizes data exchanges between systems

TSA will conduct incremental laboratory and field demonstrations with multiple solution providers at different airports and checkpoints to further mature the TRS concept. These demonstrations will evaluate performance, functionality, and scalability while establishing a cost-effective and sustainable deployment strategy. TSA will sequence these demonstrations to allow for an iterative approach to discover and correct issues. They will have minimal impact on checkpoint operations, but allow us to reduce technical and programmatic risks when scaling solutions at a later date.

TSA expects to mature and evaluate TRS concepts in partnership with industry stakeholders for select capability areas before scaling to additional solution types.

Outcome: Demonstration and evaluation of operationally viable SoS solutions, using OA principles in laboratory and field environments.

Objective 2.4: Expand enterprise-wide capabilities and standardization, collection, and management of operational data.

TSA uses multiple solutions, tools, and approaches to provide enterprise capabilities directly to the field and to collect and manage operational data in the airport environment. TSA will expand efforts to enable enterprise connectivity and standardize operational data formats and interfaces for the following capabilities:

- User Management and Authentication.
- Remote Monitoring and Maintenance.
- Predictive Maintenance.
- Configuration Management.
- Remote Updates.
- Data Collection, Management, and Distribution.
- Cybersecurity.

Outcome: Common and accessible operational data to enable advanced analytics, reporting and decision-making.

Objective 2.5: Adopt, tailor, and evolve standards across the identity management lifecycle (enrollment, proofing, vetting, and verification) to enhance security, efficiency, and user experience while preserving core values such as privacy and equity.

TSA will provide input and use standards published by the National Institute of Standards and Technology (NIST) and other reputable organizations (for example, International Organization for Standardization/ International Electrotechnical Commission) to inform requirements for the development of accurate, equitable and privacy-preserving biometric and digital identity solutions to address critical mission needs across the identity management lifecycle and use cases.

These standards (like NIST 800-63 rev 4) will guide TSA when developing governance of, and solutions for, identity management. This includes the acceptance and interoperability of identity information and documents, like physical or digital credentials, across various interfaces (for example, enrollment systems, airline/airport systems) and priority use cases for air travelers and credentialed populations.

An open, vendor-agnostic, standards-based approach will facilitate TSA solution development and governance. It will also provide clear guidance to interagency and industry partners on the development of next-generation identity solutions including enhanced biometric and digital identity capabilities (like mobile driver's license). Not only will this approach help meet TSA's mission needs by prioritizing cybersecurity and data minimization, it also provides security of data in transit and at rest.

Outcome: Industry-leading requirements, governance, and capabilities developed in coordination with interagency and industry partners to meet critical mission needs and modernize TSA-operated or regulated interfaces with standards-based biometric and digital identity solutions.

Organizational Policy and Procedures

Goal 3: Evaluate policies, processes, products, and organizational needs to support the implementation and management of open and interoperable transportation security SoS solutions.

Objective 3.1: Establish guidelines for the tailoring of acquisition activities within the Acquisition Lifecycle Framework to support the evolution of policies, processes, and activities in an OA and transportation security SoS environment.

The full benefits and capabilities of OA can only be recognized with the transition to a transportation security SoS approach to acquisitions. The acquisition methods, processes, activities and products conducted or produced must be tailored to the SoS approach and evolve with the pace of technology. TSA must innovate, develop, plan for, document, obtain, deploy, and maintain new capabilities in a rapid and efficient manner using a more modular and vendor-agnostic approach.

TSA will evaluate the current approaches and establish tailoring guidelines to enable consistent development, testing, procurement, contracting, and sustainment strategies in an OA environment. The guidelines will include considerations to analyze and tailor acquisition activities to improve TSA's ability to leverage OA capabilities and inform the products and decision-makers through:

- Early acquisition activities and products such as gap analysis, requirements development, need/capability/solution identification, capability development, demonstration processes, concept of operations and resourcing.

- Later phase activities and products to include capability/technology development, test and evaluation, procurement, deployment, maintenance and sustainment, and resourcing.

The guidelines will also address common methods and processes shared across these phases to include:

- Testing and Evaluation: Evolve and tailor current Testing and Evaluation processes, infrastructure, and strategies to support the interchangeability and interoperability capabilities in a transportation security SoS solution.
- Contracting and Procurement: Ensure TSA has the contract vehicles and procurement strategies necessary to enable the rapid establishment of flexible collaboration with industry partners throughout the capability lifecycle while protecting intellectual property in an open, transportation security SoS environment.
- Training: Update and adapt the training development and implementation processes in support of a vendor-agnostic methodology.
- Investment: Identify, tailor or establish the governance processes and authorities to approve the investment and resourcing needs as well as opportunities and trade-offs directly associated with OA.

The acquisition guidelines will establish the foundation on which TSA will begin to evolve and implement policies, processes, and solutions.

Outcome: Acquisition guidelines to advise and inform the acquisition community on the tailoring and implementation of improved policies, processes and practices across the capability lifecycle in an open, transportation security SoS environment.

Objective 3.2: Develop holistic transportation security SoS approaches to reduce complexity, increase interoperability, advance cybersecurity capabilities, streamline development, and mitigate and adapt to emerging cyber threats.

The establishment of a standards-based, transportation security SoS in which state-of-the-art solutions are quickly adopted to address emerging threats and information is shared in real time across screening solutions, requires a clear definition of the relationships between capabilities and application of advanced cybersecurity solutions.

A successful transportation security SoS approach will define an integrated environment that promotes maximum interoperability. In partnership with stakeholders, TSA will define the intermediate and long-term integrated transportation security SoS environment. With multiple viewpoints and approaches, it is essential that TSA proactively document, analyze alternatives, and implement incremental solutions while working towards long-term goals.

Cybersecurity is a growing and evolving domain that requires rigorous evaluation of risk, definition of requirements, compliance to appropriate standards, and assessments. It is critical that TSE under a transportation security SoS comply with federal cybersecurity policy including the Federal Information Security Modernization Act of 2014 (Public Law 113-283) and, as necessary, the cyber controls in NIST 800-53 and 800-82. To move towards an integrated transportation security SoS environment, TSA will improve cybersecurity throughout the design, development, and testing processes. TSA will evaluate the approach to conducting cybersecurity evaluations in a SoS environment to include software coding security.

Outcome: Holistic checkpoint architecture to guide complex transportation security SoS development and improvement of cybersecurity requirements and capabilities across the development life cycle.

Data Sharing

Goal 4: Enable rapid solution development to improve emerging threat response and adoption of best-in-class security innovations.

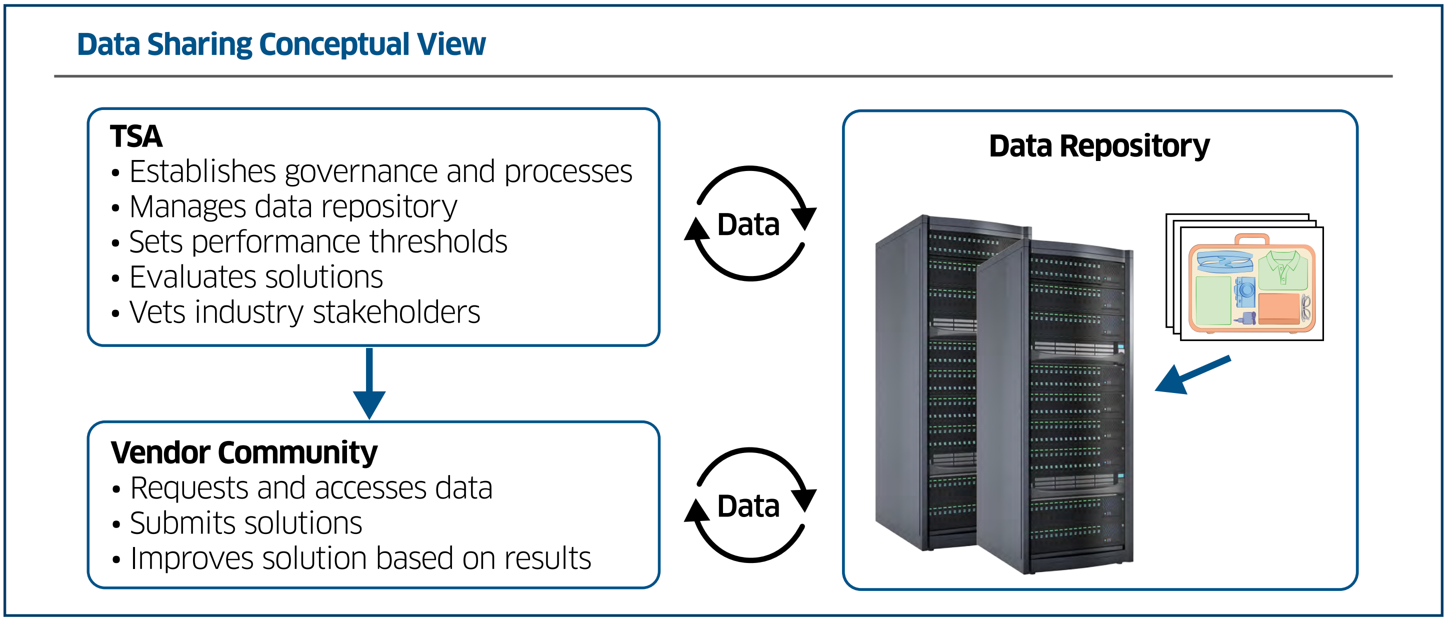
Objective 4.1: Establish a robust stream of commerce (SoC) and threat data collection, annotation, management, and distribution pipeline.

Industry guidance indicates that most algorithm development cost and resources are focused on up-front data collection and management. Therefore, TSA will institute holistic and continuous data collection, annotation, management, and distribution methodologies to enable development and testing with industry partners. Figure 6 shows TSA's conceptual data sharing view.

TSA will evaluate the approach to existing data collection initiatives by applying a "pipeline" framework. In a pipeline framework, up-front data collection decisions directly impact downstream utility of the data and vendors' ability to develop effective solutions in support of TSA's mission. This objective will increase access to relevant data sets for all industry partners, allow for industry feedback and continuous improvement of data quality, improve solution performance, and reduce costs to TSA through a unified management approach. As part of the data sharing approach, TSA will evaluate data classification and establish necessary policies to protect data privacy.

TSA has launched data collection initiatives across multiple capability areas. These initiatives support solution development, and we expect to expand them to ensure that data sets represent an operational environment. TSA will apply lessons learned to other capability areas as appropriate.

Figure 6. Data Sharing Conceptual View


Data Sharing Conceptual View
TSA
• Establishes governance and processes
• Manages data repository
• Sets performance thresholds
• Evaluates solutions
• Vets industry stakeholders
Vendor Community
• Requests and accesses data
• Submits solutions
• Improves solution based on results
Data
Data
Data Repository

Outcome: Comprehensive screening data pipeline to enable solution development in support of TSA's mission and industries' need for relevant data.

Objective 4.2: Create a transparent and continuous mechanism to develop and evaluate solutions (like algorithms or workstations) while promoting market growth and competition.

Clear and consistent guidelines and processes will enable rapid development and testing of solutions. TSA will outline the conditions in which developmental funding may and may not be provided to minimize technical and financial risks while promoting market growth and innovation. TSA aims to use robust data collection, annotation, and the management pipeline to promote continuous development and testing of security solutions. Owing to the sensitivity of the data, TSA will evaluate the suitability of each vendor and individual requesting access to data.

Outcome: Clear pathways for all industry partners to engage with TSA in support of mission objectives and appropriate data sharing to support solution development.

Path Forward

The execution of the TSA OA Roadmap will begin with the implementation of each objective as TSA progresses in establishing the foundational elements of an open, connected transportation security SoS. Figure 7 outlines the success criteria and estimated milestones for achievement of the goals and objectives. The success criteria and milestones may change as TSA partners with stakeholders on these efforts and expands on the approaches.

Figure 7. Estimated Schedule for Goals and Objectives

Number	Goal	Success Criteria	Milestone
1	Implement enhanced coordination and communication with government, industry, and stakeholder organizations at the strategic, programmatic, and technical level to build partnerships in the development of an open, connected transportation security SoS.		
1.1	Communicate and coordinate strategic and programmatic initiatives with government, industry, and stakeholder organizations and facilitate ongoing engagement.	• Publish roadmap • Host industry day • Participate in relevant events	Q4 FY23 Q4 FY23 Q3 FY24 – Q4 FY26
1.2	Implement recurring technical forums, working groups, and methodologies to enable collaboration and continuous improvement of OA technical standards and capabilities.	• Maintain DICOS working group • Establish OPSL working group	Q3 FY23 – Q4 FY26 Q4 FY24
Number	**Goal**	**Success Criteria**	**Milestone**
2	Establish and adopt OA technical standards and capabilities to enable interoperability and a flexible, plug and play screening environment.		
2.1	Adopt common and accessible data format through real-time Digital Imaging and Communications in Security (DICOS).	• Define Checkpoint CT DICOS requirements • Establish user-driven software model	Q4 FY23 Q4 FY24
2.2	Adopt common and accessible interface format through Open Platform Software Library (OPSL).	• Define Checkpoint CT OPSL requirements • Establish user-driven software model	Q4 FY23 Q4 FY24
2.3	Demonstrate a scalable and common computing platform to provide an open transportation security SoS solution.	• Conduct lab assessment • Conduct airport assessment	Q4 FY23 Q4 FY25
2.4	Expand enterprise-wide capabilities and standardization, collection, and management of operational data.	• Establish modernization approach	Q4 FY25

Number	Goal	Success Criteria	Milestone
2	Establish and adopt OA technical standards and capabilities to enable interoperability and a flexible, plug and play screening environment.		
2.5	Adopt, tailor, and evolve standards across the identity management lifecycle (enrollment, proofing, vetting, and verification) to enhance security, efficiency, and user experience while preserving core values such as privacy and equity.	• Operationalize standards for TSA	Q3 FY25
Number	Goal	Success Criteria	Milestone
3	Evaluate policies, processes, products, and organizational needs to support the implementation and management of open and interoperable transportation security SoS solutions.		
3.1	Establish guidelines for the tailoring of acquisition activities within the Acquisition Lifecycle Framework to support the evolution of policies, processes, and activities in an OA and transportation security SoS environment.	• Create TSA OA acquisition guidebook	Q4 FY24
3.2	Develop holistic transportation security SoS approaches to reduce complexity, increase interoperability, advance cybersecurity capabilities, streamline development, and mitigate and adapt to emerging cyber threats.	• Establish holistic TSA data standards • Define cybersecurity approach	Q4 FY24 Q4 FY25
Number	Goal	Success Criteria	Milestone
4	Enable rapid solution development to improve emerging threat response and adoption of best-in-class security innovations.		
4.1	Establish a robust Stream of Commerce (SoC) and threat data collection, annotation, management, and distribution pipeline.	• Establish TSA data sharing policies	Q4 FY24
4.2	Create a transparent and continuous mechanism to develop and evaluate solutions (e.g., algorithms, workstations) while promoting market growth and competition.	• Establish industry partnership strategy	Q4 FY24

Appendix: Acronyms and Glossary

Acronym	Term
ATR	Automated Threat Recognition
CBP	Customs and Border Protection
CT	Computed Tomography
DICOS	Digital Imaging and Communications in Security
DOD	Department of Defense
MOSA	Modular Open Systems Approach
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
OA	Open Architecture
OPSL	Open Platform Software Library
SoC	Stream of Commerce
SoS	System of Systems
T&E	Test and Evaluation
TRS	Threat Recognition System
TSA	Transportation Security Administration
TSE	Transportation Security Equipment
TSO	Transportation Security Officer

Term	Definition
Digital Imaging and Communications in Security	Common and accessible data file format to enable the exchange of consistent information for security screening equipment while maintaining a high level of image quality.
Open Architecture	Design approach in which equipment components, such as software and hardware, are standards-based and interoperable to allow a wide range of industry partners to create improved subcomponents.
Open Platform Software Library	Common and accessible set of Application Programming Interfaces (APIs), standardizing how software can interact with each other to enable interoperability between screening solutions.
System of Systems	Set of systems or system components that interact to provide a unique capability that cannot be accomplished independently.
Threat Recognition System	Combines the computing hardware, DICOS, and OPSL to provide a platform for integrating screening equipment, establish a scalable computing approach to leverage multiple industry partner algorithms, allow for a common workstation, and rapidly collect data.

Westin Hotel, Plaza
Transit Center
SUM MER DEN
Restricted Access
HOLD IT
REFILL IT
TSA
TSA Pre✓
ProVision ATD
STOP
Notice of Additional Screening
DO NOT REMOVE
Your safety is our priority
iLane

TRANSPORTATION SECURITY ADMINISTRATION

@TSA @TSA facebook.com/TSA