Transportation
Security
Administration

Open Architecture Strategic Roadmap

Version 0.1

February 2023

DRAFT

OPEN ARCHITECTURE STRATEGIC ROADMAP

TABLE OF CONTENTS

Administrator's Message 2
1. Executive Summary ..... **Error! Bookmark not defined.**
2. Purpose and Scope 3
3. Vision 4
   Figure 1. SoS Vision Across TSA Capability Areas 4
4. Strategic Drivers 5
5. Guiding Principles 6
   Figure 2. OA Principles Provide Flexibility to Tailor Solutions to Best Meet User Needs .. 7
6. Future State 7
7. Goals and Objectives 8
   Figure 3. OA Goals 9
   7.1 Engagement 9
   7.2 Technical Standards and Capabilities 10
   Figure 4. Adoption of Technical Standards and Capabilities 11
   Figure 5. Transportation Security System of Systems Operational View 13
   7.3 Organizational Policy and Procedures 14
   7.4 Data Sharing 16
8. Path Forward 17
9. Appendix: Terms and Acronyms 18

DRAFT

ADMINISTRATOR'S MESSAGE

February 2023

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 that can rapidly field innovative screening solutions that improve 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, it is imperative we implement innovative screening solutions in a manner that supports the Transportation Security Officer in conducting critical screening functions and improves the passenger experience. Leveraging an open architecture design approach will allow TSA to improve its security posture, support our frontline workforce, and promote an improved traveler 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 leverage strategic industry and international partnerships that allow 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 document that builds on the vision outlined in the TSA Strategy (2018 – 2026), the Administrator's Intent, TSA Innovation Doctrine, and TSA's Capability Roadmaps to provide the holistic direction to guide TSA's Open Architecture goals and objectives.

I want to thank everyone at TSA and our interagency, industry, and international partners who contributed to the development of this Roadmap. It is going to take some time to bring Open Architecture concepts to maturation, but continuing to work together we can realize this vision and improve security effectiveness and passenger experience, support TSA's frontline workforce and expand industry and international engagement. This is a global aviation security priority.

Sincerely yours,

David P. Pekoske
Administrator

DRAFT

1. INTRODUCTION

Currently, TSA's security screening system is highly complex with limited data or interface standardization. This hinders TSA's ability to rapidly field innovative screening solutions to respond to the evolving threat environment, thus presenting barriers to TSA achieving the desired security posture. Additionally, this puts an ever increasing burden on our frontline officers to perform their critical screening functions with cumbersome procedures, complex training, and varying user interfaces. Consequently, this limits TSA's ability to quickly adopt state-of-the-art solutions and streamline functionality for ease of use.

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 (e.g., new detection algorithms, user interfaces, reporting systems, etc.). Leveraging this approach will present TSA with the ability to establish a superior transportation security System of Systems (SoS) by taking a set of systems or system components that interact and provide a unique capability that cannot be accomplished independently. TSA aims to leverage the best practices of the Department of Defense (DOD) Modular Open Systems Approach (MOSA) to achieve the goals and objectives outlined in this Roadmap.

Applying an OA approach allows TSA a multitude of benefits and improves TSA's execution of the security mission, supports our frontline workforce, improves the passenger experience, and further enhances the agency's engagement with the security industry. The successful implementation of this approach will require coordination across a wide range of partners to include government agencies, regulators, industry and international partners, national labs, academia, and airports.

2. PURPOSE AND SCOPE

TSA is challenged with the need to establish a solution 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 solution cannot leverage various alternative vendor implementations as this puts significant burden on our frontline workforce to endure the variation across configurations and puts TSA in a position to operate as integrator. It is imperative that the solution be standards-based and allow for partnerships across the security industry while providing the frontline with the tools they need to perform the mission.

The purpose of this Roadmap is to serve as a foundation for providing TSA's vision, goals, and objectives to establish a connected transportation security SoS, leveraging OA guiding principles. This Roadmap will guide TSA's OA activities and identify short-term (within three years) and long-term (3+ years) needs to sustain success. We intend for the Roadmap to evolve and create more detailed artifacts as TSA partners with industry and stakeholder organizations to implement OA goals and objectives.

DRAFT

3. 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 enable a dynamic screening environment. This vision outlines TSA's commitment to our most important asset, the dedicated frontline officers securing the transportation system, to provide the best tools to conduct mission critical screening operations while simplifying operational processes and procedures. Figure 1 illustrates this vision encompasses the combination of people, processes, and technologies across several capability areas to include identity verification, accessible property screening, on-person screening, checked baggage screening, and alarm resolution.

Figure 1. SoS Vision Across TSA Capability Areas

4. STRATEGIC DRIVERS

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

- **Improve Security Effectiveness:** TSA must be proactive in our approach to addressing the threat. This requires the ability to rapidly respond to emerging and evolving threats to the mission. An approach is needed to introduce improved and multiple algorithms, user interfaces, or other potential solutions to the screening environment faster and with greater flexibility (e.g., plug and play). By leveraging OA principles, we increase the ability to deliver enhanced people, 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 variability in the Transportation Security Equipment (TSE) has resulted in significant complexity in the TSA screening mission. This complexity is evident by the various user interfaces, training, and procedures required to utilize the different types of equipment. It is critical that the collective transportation security system of people, processes, and technology be taken into account and TSA focus on the 55,000 dedicated TSOs to ensure the processes and technology are optimized for the people in performing the mission. This means focusing on simplifying technology and processes, standardizing user interfaces, and rapidly responding to end user needs.

- **Improve Operational Efficiency:** TSA needs to optimize the use of the TSE to increase overall capacity of the transportation security SoS. As passenger volumes increase, the available space to conduct current screening approaches will not keep pace. It is critical that TSA leverage OA principles to drive solutions to reduce false alarms, improve TSO performance through simplifying the screening process, and establish capabilities for improving overall TSE use (e.g., remote screening).

- **Improve the Passenger Experience:** TSA needs to support screening 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 luggage when traveling abroad. Applying risk-based methodologies will provide a tailored screening approach for passengers, resulting in an overall improved screening experience. As TSA implements innovative industry solutions, we expect passengers will encounter fewer false alarms on their person and/or baggage, resulting in fewer pat-downs and bag searches, further improving the overall experience.

- **Expand Industry and International Engagement:** TSA strives to support multiple pathways and international coordination for a diverse marketplace to participate in the development and deployment of security capabilities. By leveraging OA principles, TSA is able to implement multiple awards and acquisitions targeted to specific components of

DRAFT

the system that reduce the risks and up-front investment (i.e., lowers the barrier to entry) associated with delivering a complete solution for a single award. In addition, industry partners can more easily participate within different segments of the market depending on their business model. TSA has an uncompromising interest in ensuring all industry partners – Original Equipment Manufacturers (OEM), third party, and otherwise – have their Intellectual Property (IP) protected to encourage a diverse and growing market. While IP rights are legally protected, TSA will work with industry partners to help implement reasonable technical solutions to ensure IP protection. Additionally, OA is a global aviation security priority, and TSA is focused on collaborating with international and government partners to improve aviation security worldwide. OA provides multiple opportunities for partners to share in development activities and fosters joint capability implementation.

- **Increase Cybersecurity:** Cybersecurity requires rigorous and ongoing evaluation of risk and threats, definition of requirements, compliance with appropriate standards, and assessments to mitigate cyber vulnerabilities. To move toward a complete implementation of capabilities in an integrated, networked transportation security environment, TSA must incorporate 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 execute their functionality. To realize the full benefits of OA, TSA must work within the acquisition framework to tailor acquisition activities and strategies enabling TSA to develop, test, deploy, and maintain new capabilities in a rapid and efficient manner using a more modular and vendor-agnostic SoS approach.

- **Improve Data Analytics and Decision-making:** Moving toward an open, connected transportation security SoS allows for standardized critical data elements and collection of relevant information for analytical purposes to support 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.

5. GUIDING PRINCIPLES

With OA being a design approach, or methodology, it provides the following guiding principles 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 and industry stakeholders.

DRAFT

- **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 and mobile phones were limited in their ability to rapidly implement new capabilities. As television and mobile phone designs continued to become standardized and more modular, this presented a level of future-proofing in which a user is provided a familiar interface while being able to tailor the experience for changing needs (e.g., cable boxes, disc players, software applications).

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

6. FUTURE STATE

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

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

DRAFT

- **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 and implement solutions for officers, share information in real time for backend development and analytical purposes, 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 step to realize an open, connected transportation security SoS, there is a need to evaluate current operating models, policies, processes, and resourcing to ensure an effective long-term, sustainable strategy that aligns with internal and external stakeholders. TSA understands the strategy, objectives, and goals outlined in this Roadmap are not without challenges. TSA will evaluate and adapt to take advantage of OA capabilities and will incrementally evolve existing policies and processes in collaboration with government partners and industry stakeholders to minimize risk and apply lessons learned.

- **Data Sharing:** Technical standards and capabilities enable the ability to obtain data and support rapid development of new algorithms or other solutions. To capitalize on this, 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, government partners, and industry stakeholders will work in partnership to define appropriate data collection, annotation, storage, and distribution methodologies to support data security, cost efficiencies through shared data models, and industry growth.

7. 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. The cross-cutting nature of the goals and objectives across TSA's mission capability areas requires incremental introduction of solutions into each capability roadmap. Each policy, process, and solution is expected to continually evolve in support of TSA's mission as TSA and industry stakeholders 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 their development of solutions. Figure 3 illustrates TSA's vision and goals around 1) engagement, 2) technical standards and capabilities, 3) organizational policies and procedures, and 4) data sharing.

DRAFT

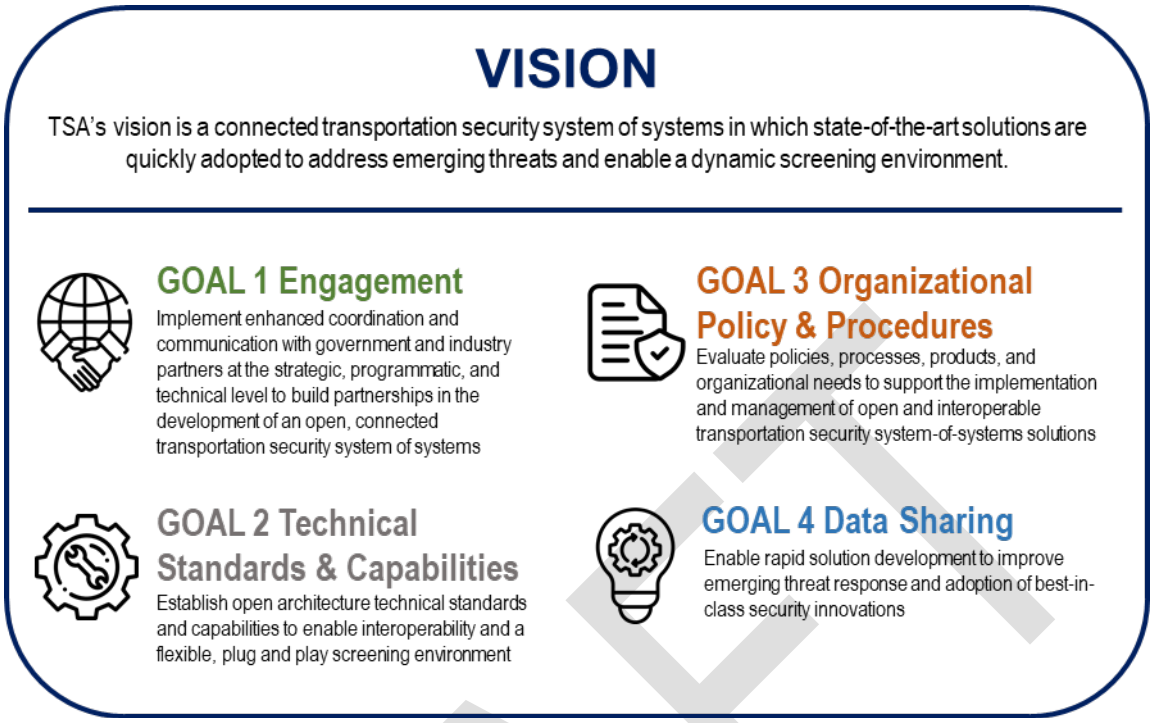

Figure 3. OA Goals

7.1 Engagement

Goal 1: Implement enhanced coordination and communication with government and industry partners 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 and industry stakeholders and facilitate ongoing engagement.

TSA will continue to outline the vision, goals, objectives, and any deviations from this Roadmap as more is learned through implementation. TSA expects this Roadmap may need to be updated and could support development of more detailed artifacts. TSA will communicate major updates to overall strategy to industry in a consistent TSA voice to ensure effective policy development and interpretation.

Multiple combinations of stakeholder solutions are required to achieve a connected transportation security SoS. TSA will partner with government and industry stakeholder organizations to promote transparent communication of initiatives as appropriate throughout the development, demonstration, and implementation process to showcase progress, enable adoption of successful solutions, and incorporate lessons learned into the development process as the collective stakeholder community works toward a connected transportation security SoS, leveraging OA principles. TSA will also establish a comprehensive field engagement strategy to ensure successful implementation of adopted solutions. TSA will leverage the experience, capabilities, and authorities of other government agencies with shared goals and collaborate with

DRAFT

industry to achieve a system that considers industry needs while maintaining and/or enhancing TSA's ability to carry out its mission.

As an example, TSA is focused on supporting the efforts with international and government partners to ensure a collaborative move toward improved security such as the One-Stop Security initiative. One-Stop Security is a partnership with TSA, DHS Customs and Border Protection (CBP), and several domestic and international partners to work towards a security solution with the potential to alleviate rescreening luggage when traveling into the United States and abroad. This focus is balanced with the need to ensure TSA's implementation drives toward a connected transportation security system that meets the needs across the 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 and industry stakeholders to collaborate on the adoption and maintenance of approved technical standards and capabilities. TSA understands that an open, connected transportation security SoS is never complete and must continue to evolve over time. Technical forums and working groups allow TSA and industry subject matter experts 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 OA solutions to help provide a unified market for aviation security equipment and reduce variation and complexity for industry in their development of solutions.

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

7.2 Technical Standards and Capabilities

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

DRAFT

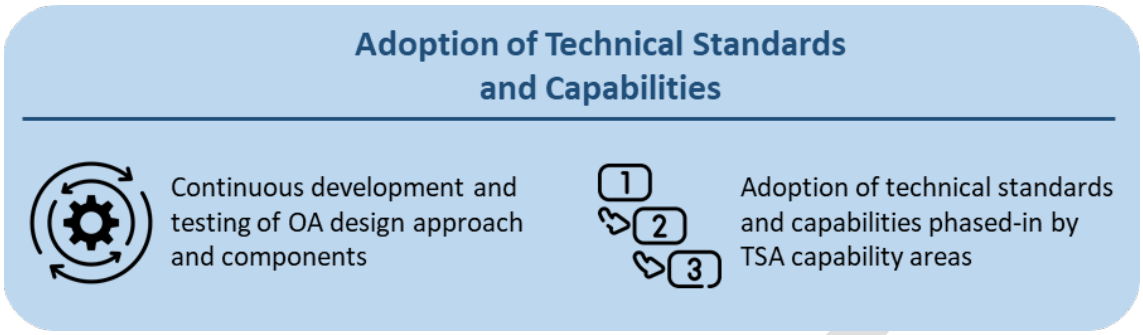

Figure 4. Adoption of Technical Standards and Capabilities

Goal 2: Establish 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).

The DICOS standard provides a 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. TSA will implement real-time DICOS for screening solutions to leverage the consistent information exchange 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. DICOS was established in 2009 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 and valuable lessons learned for TSA and industry to apply to the security screening domain.

TSA expects to initially adopt real-time DICOS for accessible property screening (APS) solutions (i.e., Checkpoint Computed Tomography (CT)) before moving on to additional capability areas as appropriate while applying lessons learned.

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 and accessible set of Application Programming Interfaces (APIs), standardizing how software can interact with each other to enable interoperability between screening solutions. TSA will implement OPSL for screening solutions to enable systems and system components to share and move data consistently across the SoS. OPSL will enable an interoperable SoS in which TSA and industry partners can more easily incorporate new solutions into the screening environment. As TSA adopts OPSL, OPSL 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

DRAFT

future where OPSL is maintained and matured through a collaborative effort with all of industry and has only a level of governance to ensure releases are available to all of industry.

In this model, TSA facilitates:

- which features and updates are prioritized and approved.
- 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 leverage open-source software development methodologies and industry best practices and talent to continuously develop, test, and maintain OPSL long-term. Additionally, a user-driven model provides industry with maximum code transparency to adapt their capabilities to be OA compliant and is designed to improve code at a tempo consistent with TSA mission and industry needs.

TSA expects to initially adopt OPSL in a limited capacity for APS solutions while, in parallel, 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 leveraging DICOS and OPSL. Figure 5 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, establish a scalable computing approach to leverage multiple industry partner algorithms, and allow for a common workstation. The TRS approach mitigates potential cybersecurity vulnerabilities by providing a common operational solution to minimize the threat space 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.

DRAFT

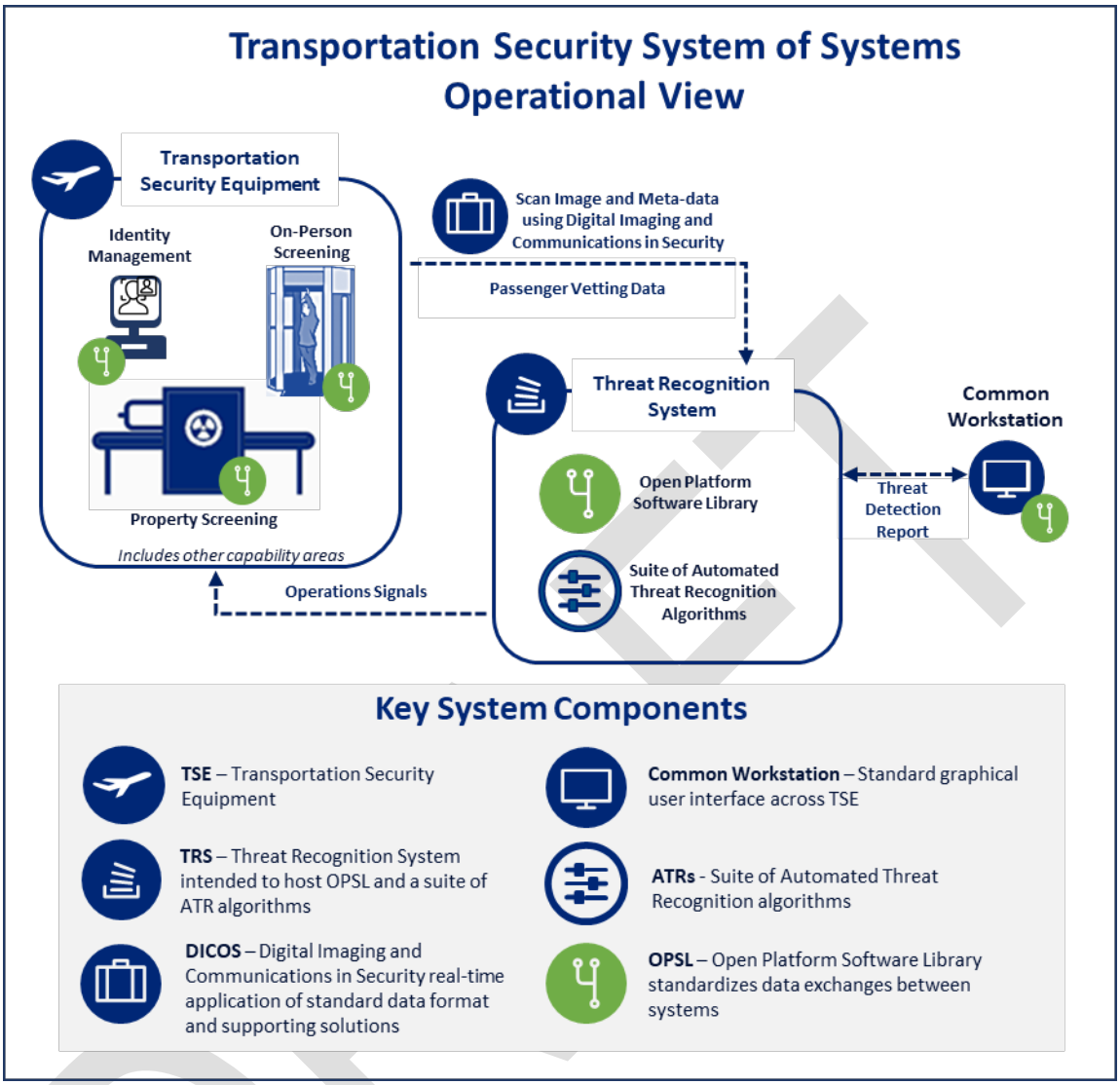

Figure 5. Transportation Security System of Systems Operational View

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

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

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

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

TSA currently uses multiple solutions, tools, and approaches to provide enterprise capabilities directly to the field and collect and manage operational data in the airport environment. TSA will expand existing efforts across the transportation security SoS and prioritize standardization of operational data formats and interfaces with the enterprise. TSA will focus on the following capabilities to enable enterprise connectivity with the transportation security SoS solutions:

- 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 and decision-making.

Objective 2.5: Adopt, expand, and evolve standards across the identity, enrollment, proofing, vetting, and verification lifecycle.

TSA will continue to leverage standards generated by the National Institute of Standards and Technology (NIST) and other reputable organizations to develop 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 standards will facilitate industry's ability to develop new biometric capture or digital identity products and solutions that meet TSA's future goals while prioritizing information and data security.

Outcome: Industry flexibility to establish digital identification while ensuring compatibility with TSA's identity verification solutions.

7.3 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 methods, processes, activities and products conducted or produced must be tailored and evolved with the pace of technology. TSA

DRAFT

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 tailor strategies and processes for the following acquisition activities and specific topic areas to improve TSA's ability to leverage OA capabilities and inform the products and decision-makers:

- Analyze and tailor early acquisition activities and products to include, but not limited to, gap analysis, requirements development, need/capability/solution identification, capability development, demonstration processes, Concept of Operations and resourcing.

- Analyze and tailor 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 (T&E): Evolve and tailor current T&E 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 IP 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 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 upon which TSA will begin to evolve, tailor, 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.

DRAFT

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 to mitigate cyber vulnerabilities. It is critical for TSA to ensure compliance with the Federal Information Security Modernization Act (FISMA) and to implement cyber controls per the NIST 800-53 and 800-82 for Transportation Security Equipment under a transportation security SoS environment. To move towards an integrated transportation security SoS environment, TSA will incorporate cybersecurity throughout the design, development, and testing processes.

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

7.4 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 the majority of algorithm development is focused on the up-front data collection and management. Therefore, TSA will institute holistic and continuous data collection, annotation, management, and distribution methodologies and solutions to enable development and testing with industry partners. TSA will evaluate the approach to existing data collection initiatives with an emphasis on applying a "pipeline" framework in which 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, improve solution performance, and reduce costs to TSA through a unified management approach.

TSA has launched data collection initiatives across multiple capability areas to support solution development and expects to expand existing activities to ensure data sets are representative of an operational environment. TSA will apply lessons learned to other capability areas as appropriate.

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

DRAFT

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

Clear and stable 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 the technical and financial risks while promoting market growth and innovation. TSA aims to leverage robust data collection, annotation, and the management pipeline to promote continuous development and testing of security solutions in support of TSA's mission. Considering 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.

8. PATH FORWARD

The execution of the TSA OA Strategic Roadmap will begin with the implementation of each objective as TSA progresses in establishing the foundational elements of an open, connected transportation security SoS. The expectation is the Roadmap will mature into more detailed artifacts. This will enable TSA to evolve and incorporate lessons learned through the implementation. The achievement of the vision, goals, and objectives outlined in this Roadmap will require close coordination and collaboration across government and with domestic and international stakeholders, regulators, industry, national labs, academia, and airports.

DRAFT

9. APPENDIX: ACRONYMS AND GLOSSARY

Acronym	Term
API	Application Programming Interface
APS	Accessible Property Screening
ATR	Automated Threat Recognition
CBP	Customs and Border Protection
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
DICOS	Digital Imaging and Communications in Security
DOD	Department of Defense
FISMA	Federal Information Security Modernization Act
IP	Intellectual Property
MOSA	Modular Open Systems Approach
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
OA	Open Architecture
OEM	Original Equipment Manufacturer
OPSL	Open Platform Software Platform
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.