International Civil Aviation Organization
North American, Central American and Caribbean Office

INFORMATION PAPER

NACC/DCA/14 — IP/15
15/05/26

Fourteenth Meeting of the North American, Central American and Caribbean Directors of Civil Aviation (NACC/DCA/14)

St. George's, Antigua and Barbuda, 1 to 5 June 2026

Agenda Item 5: Every Flight is Secure

ADVANCING THE U.S. TRANSPORTATION SECURITY ADMINISTRATION (TSA) OPEN ARCHITECTURE FOR AVIATION SECURITY SYSTEMS

(Presented by United States)

EXECUTIVE SUMMARY

This Information Paper provides an overview of the U.S. Transportation Security Administration's (TSA) Open Architecture (OA) initiative and proposes actions to promote common data standards and collaboration.

Strategic Objectives:	• Every Flight is Safe and Secure
References:	• ICAO Annex 17 – *Aviation Security* • ICAO Aviation Security Manual (Doc 8973) • ICAO Aviation Cybersecurity Strategy • ICAO Cybersecurity Action Plan

1. Introduction

1.1 On 31 July 2023, the United States published the Transportation Security Administration (TSA) Open Architecture (OA) initiative and roadmap, which outlined success criteria and milestones to support the achievement of its goals and objectives toward an open, connected transportation security System of Systems (SoS).[1]

1.2 The TSA mission is to protect U.S. transportation systems to ensure the freedom of movement for people and commerce. TSA prioritizes being an agile and flexible organization that can rapidly evaluate and deploy new screening solutions capable of improving the network's security posture while maintaining commitment to TSA's frontline workforce and the traveling public. To accomplish this, TSA implements innovative screening solutions in a manner that supports the Transportation Security Officer (TSO) in conducting critical screening functions, improves screening efficiency, and enhances the passenger experience.

[1] https://www.tsa.gov/sites/default/files/oa_roadmap_20230717_508c-r1.pdf.

1.3 Using an OA design approach enables TSA to achieve these objectives while also improving the overall security posture. The OA design approach is founded on the concept of ensuring that transportation security equipment (TSE) components, such as software and hardware, are standards-based and interoperable. This affords TSA the ability to leverage strategic industry and international partnerships to facilitate the adoption of increasingly interconnected technologies and processes while employing advanced cybersecurity capabilities. OA expands TSA's engagement with innovative partners, such as small businesses and academic institutions, while maintaining relationships with traditional industry vendors.

2. Background

2.1 Open Architecture (OA) is a design approach where equipment components are standards-based, interoperable, and use non-proprietary formats and interfaces accepted by the aviation security industry. This enables broader industry participation, fosters innovation, and allows TSA to integrate diverse systems for enhanced transportation security—capabilities not achievable by a single vendor. TSA is also working with international partners to align OA solutions globally, promoting a unified market and reducing complexity in aviation security equipment development.

2.2 TSA has a history of advancing OA concepts dating back to 2010, when TSA worked in partnership with industry to establish the first security image data standard. TSA has subsequently continued to support the maturation of this standard through three formal updates. TSA has accelerated its efforts related to OA and is taking 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.

2.3 The successful implementation of this approach requires coordination across a wide range of partners like government agencies, stakeholder organizations, industry and international partners, national labs, academia, airlines and airports. TSA uses the best practices of the U.S. Department of Defense (DOD) Modular Open Systems Approach (MOSA) to achieve the goals and objectives outlined in TSA's OA Roadmap.

3. Discussion

Strategic Drivers for TSA's OA

3.1 The following strategic drivers are the catalysts for defining and pursuing TSA's OA goals and objectives.

a) **Improve Security Effectiveness and Agility**: TSA must be able to proactively identify, assess, and mitigate security threats. 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 with greater speed and 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. These principles support establishing a future-ready transportation security SoS that is more effective and builds TSO trust in the systems' performance.

b) **Support the Frontline Workforce**: The variety of 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 considered 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 (TSO) needs.

c) **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 cannot keep pace. Therefore, TSA must deploy 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).

d) **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 TSA's One-Stop Security pilot initiative, that will potentially alleviate the need to rescreen passengers and baggage when traveling into and out of the United States. By applying risk-based screening and innovative industry solutions, TSA aims to reduce false alarms and unnecessary searches, resulting in a more streamlined and positive passenger experience.

e) **Expand Industry and International Engagement**: A diverse marketplace is essential for advancing TSA's security mission, and Open Architecture (OA) drives innovation by enabling multiple contract awards for specific system components, lowering barriers to entry and encouraging broader industry participation. TSA supports OA solutions that protect intellectual property and promote usability across mission spaces, while collaborating with international and government partners to enhance global aviation security through shared development and joint implementation.

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

g) **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.

h) **Improve Data Analytics and Decision-making**: An open, connected transportation security SoS allows for standardized critical data elements and the 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.

TSA's OA Guiding Principles and Goals

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

a) **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.

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

3.3 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. To achieve this vision, TSA established the following OA goals:

a) **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 SoS.

b) **Goal 2 - Technical Standards & Capabilities**: Establish and adopt OA technical standards and capabilities to enable interoperability and a flexible, plug-and-play screening environment.

c) **Goal 3 - Organizational Policy & Procedures**: Evaluate policies, processes, products, and organizational needs to support the implementation and management of open and interoperable transportation security SoS solutions.

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

4. Conclusion

The future of the aviation ecosystem is contingent upon interoperability as design approach to accelerate innovation and increase resilience while maintaining robust cybersecurity. Interoperability can be achieved by the development and adoption of common data standards, reference architectures, Application Programming Interfaces, and shared test/evaluation methods. TSA encourages NACC States to contribute to OA efforts to enhance regional resilience and innovation.

— END —