The System Architecture (SA) allows the Transportation Security Administration to proactively define targeted screening capabilities at a **system level** and ultimately enable an **integrated, interoperable, and modularized aviation security screening system.**

### Current Challenges
The current state TSA security capability development/acquisition approach poses several challenges such as:
- Long systems/solutions development lead times
- Unique/proprietary systems designs
- Competition and innovation barriers
- Costly security suite upgrades
- Limited ability to share threat, passenger, and risk information

### Proposed Solutions
TSA SA enables:
- **Transportation Security Equipment (TSE) disaggregation** that provides the flexibility to implement new sensor components and algorithms for greater security screening.
- **Real-Time Threat Information Sharing** that allows threat information to be gathered, analyzed, and shared with enterprise systems and between TSE.

### Benefits to TSA and Industry

**Enables Modularity**
Introduces modular components by defining system infrastructure and interfaces enabling plug-&-play functionality and increasing system flexibility.

**Advances Risk Based Screening (RBS)**
Enables RBS by developing a common data model and the infrastructure required for the masking of sensitive information and use of threat data to expedite the screening process.

**Reduces Costs**
Promotes interoperability and incremental upgrades to reduce duplicative development and testing requirements.

**Enhances Innovation**
Drives standardization and modularity to foster greater competition at sub-system levels, expand industry base, and reward modular implementation via incentive-based procurement.

**Expedites Delivery of Capabilities**
Reduces the timespan between the inception and delivery of a capability by providing vendors with well-defined open standards.
System Architecture’s **strategic and tactical initiatives** have achieved key accomplishments since their commencement and continue advancing towards the development of an open, integrated security screening architecture.

### TSA System Architecture

**Initiative**

- **Open Security Screening Architecture (OSSA)**
  Support RBS strategy through end-to-end screening SA development.

- **Transportation Security Equipment (TSE) Requirements Analysis Platform (TRAP)**
  Implement SA testbed to support architectural requirements validation and capability implementation within an integrated system-of-systems.

- **Open Threat Assessment Platform (OTAP)**
  Develop an open architecture TSE prototype to allow for 3rd party detection algorithms & specialized hardware on screening technology.

- **Common GUI Displays (CGUI)**
  Develop common display standards for imaging-based TSE.

**Accomplishments**

- Current & Future State Architectures
- Interface & data standards report to enable modularization
- Roadmap depicting path towards an open system architecture
- Built on STIP Open Architecture Principles
- Core Capability of TRAP Infrastructure
- Component-based Architecture Support
- Open Platform Software Library
- 3rd Party Algorithm & Hardware
- Advanced DICOS through real-life experimentation and exercises
- CGUI technical roadmap
- EDS CGUI display prototype
- DICOS Toolkit

**Future Focus**

- Mature Concepts & Gain Consensus
- Solution Architecture
- Risk Scoring Engine
- Threat Data Engine
- Common Graphical User Interface Assessment Tools
- Testbed Operationalization
- Software release for AT
- Software development and release for CT
- Common data and network standards
- Expansion to other security technologies

---

**TSA System Architecture Project Landscape**
Transitioning to an Aviation Security Architecture (ASA)

As the organization expands from focusing primarily on technology solutions to a more holistic requirements and capabilities analysis, an adaptable and flexible integrated mission architecture will facilitate strategic decision-making by enabling the centralization and flow of agency-wide data to inform risks, prioritize requirements, and optimize budgetary and resource allocation strategies.

The Benefits & Impacts of the ASA

Enhanced Transparency

Provides transparency into activities across the aviation security ecosystem resulting in opportunities to streamline and optimize cross-cutting initiatives.

Optimized Information Exchanges

Drives efficiency into information sharing and decision-making by serving as a platform to coordinate activities across the agency.

Defined Roles & Responsibilities

Improves integration across a diverse host of stakeholders from the aviation security system, both within and external to TSA, by delineating security roles and establishing well-defined responsibilities.

Improved Risk & Vulnerability Analysis

Enhances the current state by organizing existing assets (i.e., models, databases, etc.) and current agency-wide capabilities into a common framework to quickly pinpoint system vulnerabilities and proactively adapt to emerging threats.

Generating the power to guide efficient and effective organizational decision-making
Layers of the Security Screening System (Notional)

An aviation security architecture would leverage capabilities across TSA to enable the flow and use of risk and operational information to proactively adapt to emerging threats through a comprehensive view of the security landscape.
The Approach to Defining, Designing, and Implementing The ASA

Over the next two years, TSA will continue to develop the integrated architecture through the five phases highlighted below while leveraging lessons learned from the Domestic Nuclear Detection Office (DNDO) Global Nuclear Detection Architecture (GNDA) and efforts of other government entities.

### Phase 1
Approx. 2 months
- **Solidify a Vision & Build a Team**
  - Socialize the concept of the ASA
  - Identify & obtain appropriate resources for the ASA Task Force
  - Develop a shared vision for the ASA

### Phase 2
Approx. 6 months
- **Assess the Current State & Begin Strategic Planning**
  - Begin surveying for current tools and capabilities across TSA
  - Review existing current state assessments and architectural programs
  - Develop a strategic plan to determine the path forward for the ASA

### Phase 3
Approx. 12 months
- **Begin the Design & Start Implementing**
  - Decompose the strategic plan into segment architecture artifacts
  - Conduct gap analysis to identify high-priority needs
  - Socialize the plans for enterprise-wide integration

### Phase 4
Approx. 48 months
- **Execute**
  - Implement across programs and the enterprise
  - Design and implement change management across the enterprise

### Phase 5
Ongoing
- **Sustain & Improve the Architecture**
  - Perform continuous assessments and improvements

---

**Industry Engagement**

TSA plans to collaborate, socialize, and cooperate with industry across all phases of the ASA efforts.
Questions?
Appendix
TSA System Architecture’s Five-Year Strategic Roadmap

TSA continues to pursue advanced concepts and capabilities to enable TSA’s vision of the future of aviation security screening. The System Architecture program will allow for the integration of technology, data, and processes to enable expanded implementation of risk-based security through the development of an interoperable and modularized security screening system.
TSA has partnered with a Federally Funded Research and Development Center (FFRDC) to develop the end-to-end screening system architecture. The future state of the System Architecture will allow information to be gathered, analyzed, and stored at the enterprise level and publish threat analysis locally to Transportation Security Equipment (TSE).

Gather data from TSE, intel, and external sources to provide risk information about passengers and their divested items.

Analyze source data and identify threat information to be published to appropriate systems and officers for corrective actions.

Respond to threat information received and track corrective actions taken.

Real-Time Passenger Threat Information Sharing Between Security Screening Systems

Ticket purchase → Check-in → Behavior Detection → Checked Baggage → Checkpoint

Open Security Screening Architecture - Concept Overview
TSA has begun the development of a System Architecture testbed to support architectural requirements validation and capability implementation within an integrated system-of-systems. The TSA Requirements Analysis Platform (TRAP) aims to develop a rapid prototyping/integration environment to explore and validate new architectural concepts that would enable TSA to:

- Rapidly assess capabilities/requirements and redirect technology investments
- Demonstrate and validate architecture, operations, capabilities & performance
Open Threat Assessment Platform - Proof-of-Concepts Overview

TSA is exploring proofs-of-concepts to understand how open architecture TSE prototypes can be used to implement 3rd party detection algorithms, software, and specialized hardware on screening technology. The Open Threat Assessment Platform (OTAP) is in the progress of developing and demonstrating an open architecture screening prototype in partnership with security technology manufacturers.

<table>
<thead>
<tr>
<th>Core OTAP Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open Platform Software Library (OPSL)</strong></td>
</tr>
<tr>
<td>A set of open, commonly available, and standardized data interfaces, exchanges, and formats. OPSL will serve an interface to enable engineering of 3rd party components.</td>
</tr>
<tr>
<td><strong>Passenger Baggage Object Database (PBOD)</strong></td>
</tr>
<tr>
<td>A single repository of X-Ray-scanned outputs of potential threats identified based on intelligence and analysis; information on non-threats; and any associated metadata that can be used to train algorithms for vetted vendors.</td>
</tr>
<tr>
<td><strong>Automatic Threat Recognition Algorithm Integration</strong></td>
</tr>
<tr>
<td>A set of software applications that process the various signal outputs of the X-Ray scanner to provide assisted or automated decision-support information to TSOs.</td>
</tr>
<tr>
<td><strong>3rd Party Hardware Component Integration</strong></td>
</tr>
<tr>
<td>Integration of 3rd party specialized hardware component on an OTAP-enabled system that could be potential upgrades to existing screening equipment that may provide greater security performance.</td>
</tr>
</tbody>
</table>

The OTAP project enables new solutions developed by industry (OEM and 3rd parties) by creating the tools to implement an open system architecture.
I. **Desired Outcome:** A more diverse, agile market of vendors who develop security capabilities at a much faster rate because they can specialize, spend less on integration, and easier access to test/training data.
   - Means: a) An Open System Architecture (OSA) that decouples software and hardware on TSE; b) Non-proprietary threat dataset accessible by new market entrants; c) T-BAA as transition vehicle for OTAP products

II. **Project Approach:** A structured, interactive approach provides industry with the necessary standards and development tools in an efficient and market enabling manner.
   - An integrative presence is needed to pull existing accomplishments together to achieve a strategic outcome. Piecemeal approach unlikely to produce results

III. **Partnership Approach:** FFRDC as locus for vendor-neutral, structured support of industry product development.
   - As an FFRDC, Sandia poses no threat to vendor commercial interests and can adjudicate cross-vendor technical issues more objectively than other organizational alternatives.
   - FFRDC status mitigates concerns about IP: Vendors are sharing proprietary information freely with Sandia since Sandia poses no competitive threat.

IV. **Technical Execution:** Validate through spiral development with vendors and be an integrative locus for the industry community within TSA’s System Architecture approach.
   - Cross-vendor technical issues can be analyzed in a business-safe environment.
   - OPSL needs to be validated by directly implementing the software and industry capabilities (e.g. ATR) on OEM machines.
TSA has continued to invest in and socialize the Digital Imaging and Communications in Security (DICOS) Standard, related software library, and conformance testing suite to enable airport security devices to connect over a local area network with a common format for image and metadata.

**DICOS Overview**

National Electrical Manufacturers Association (NEMA) has developed the DICOS Standard to address the exchange of digital information between security-imaging equipment and other systems.

DICOS is a standard that specifies an extensible, interoperable data format that enables the integration of security screening technologies across multiple vendor platforms and facilitates wider participation in the development of improved security screening technologies and algorithms.

**DICOS Toolkit**

- The DICOS toolkit aims to support the establishment of a common data interchange protocol and extensible file format to facilitate data information exchange
- The DICOS toolkit is provided by the TSA to vendor community free of charge to test-out the toolkit and provide feedback to the development team

- Provide a software toolkit that allows ease of DICOS implementation to reduce training and operational cost
- Support the vision of enabling an integrated, interoperable, and modularized aviation security screening system

DICOS has gained increasing acceptance as the governing committee developed and released DICOS v2A on May 15, 2017 through NEMA.
How does System Architecture change future technology?

TSA is looking to standardize the GUI on TSE such as EDS and AT which currently varies by OEM. Benefit:
• Enhance TSO performance
• Reduce operations training

TSE disaggregation allows 3rd party to develop new sensors or algorithms that can be plugged into TSE. Benefits:
• Foster greater vendor competition, enhance innovation, and expedite capability delivery by expanding market/vendor base.
• Provides the flexibility to implement new sensor components and algorithms for greater security screening.

A set of open, commonly available, and standardized data interfaces and formats developed by TSA. Benefits:
OPSL will serve as an interface to enable engineering of 3rd party components

Image of IDSS Detect 1000 provided by IDSS