Office of Security Capabilities
System Architecture

Advanced Development for Security Applications (ADSA 15)

★ ★ ★ ★ ★ ★

November 15, 2016

Keith Goll
Senior Technical Advisor
keith.goll@tsa.dhs.gov
571-227-1035

Transportation Security Administration

So what? Who cares?

The OSC System Architecture (SA) allows OSC and TSA to proactively define targeted screening capabilities **at a system level** and ultimately enable an **integrated, interoperable, and modularized 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

OSC Open System Architecture that 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.

OSC SA Ongoing Efforts

Architecture Development

Establish Current State Architecture, Future State Architecture, Gap Analysis, and Implementation Roadmap to guide TSA through Open Architecture transition.

Testbed Development

Implement system architecture testing environment to validate architectural requirements and integration of new capabilities and technologies, (e.g., **TSE Requirements Analysis Platform)**.

Prototype Software

Conduct R&D to explore the concept of Transportation Security Equipment modularity to lay the foundation for an open architecture that supports further innovation (e.g., **Open Threat Assessment Platform**).

Benefits to Industry

1. Common standards, and functional definitions
2. Common basis for comparing design alternatives
3. Industry involvement in standardization effort
4. Greater competition at sub-system level
5. Incentive-based procurement that rewards modular implementation

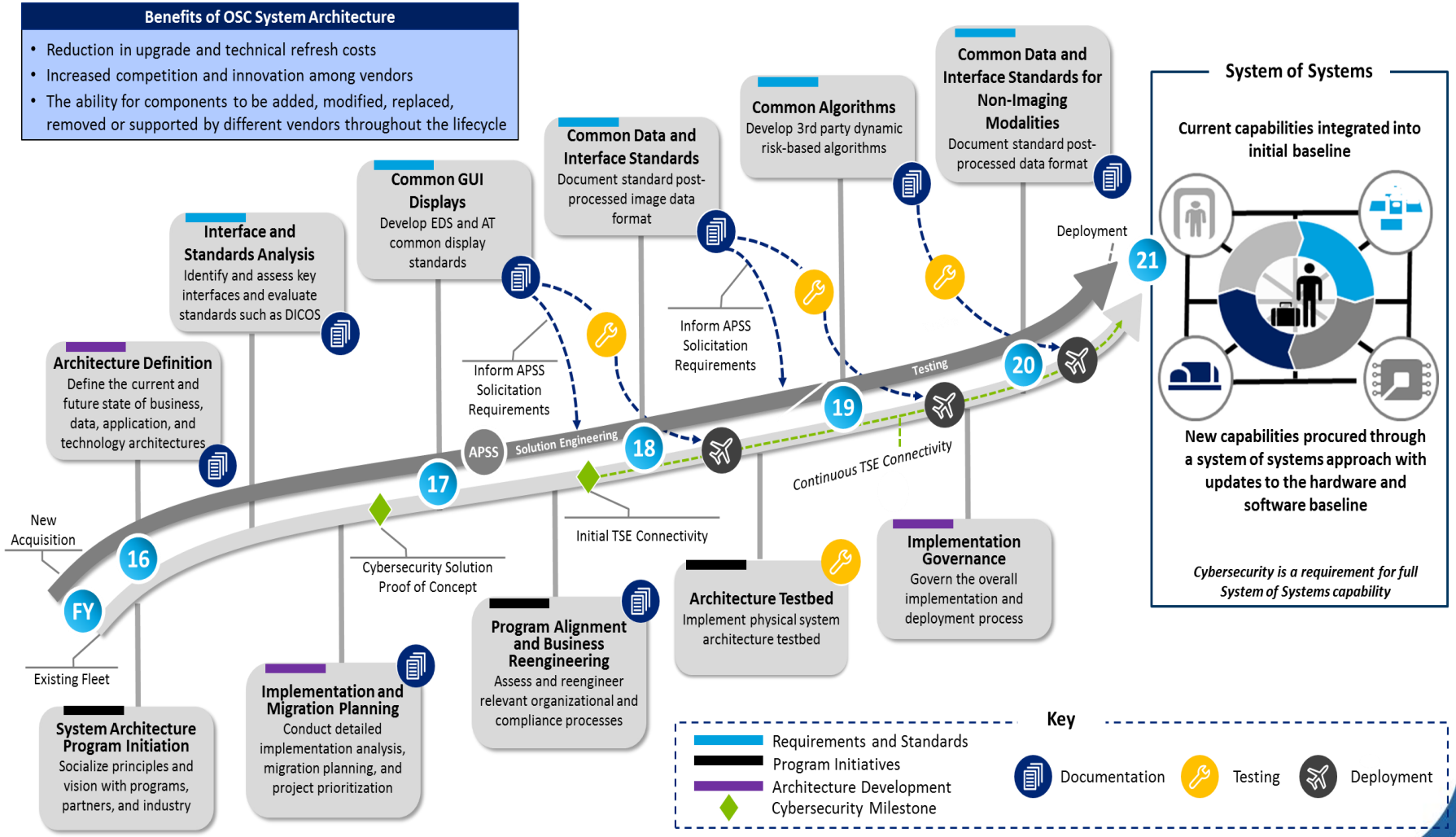
What's our future vision for aviation security?

Leadership from across TSA held a strategy session **to inform cross-cutting initiatives, drive agency alignment, and guide future organizational investments.** The 'passenger journey' framed the conversation, with new, integrated capabilities being discussed as they apply throughout eight distinct security phases.

Passenger Journey Security Screening

Security Phases		Security Capabilities
Pre-Screen	High-level vetting creates a basic risk profile when a passenger books a flight, creating risk-view of the airport population.	Identity Management, Surveillance
Perimeter	Screening takes place on a broad scale from the moment passengers and vehicles enter airport property.	Contactless Screening, Surveillance, Physical Security
Curb/Entry	Screening targets vehicles and passengers approaching the curb. Airport structures are protected from explosives and other threats.	Contactless Screening, External Partner Connectivity, Identity Management,
Check-in	Passenger risk identities are tied to bags and adversaries are prevented from bag separation.	Identity Management, Surveillance
Checked Baggage	Baggage is screened at the same level across airports. Positive bag ID means alarms in one area trigger screening at the other.	Identity Management, Surveillance
Checkpoint	Passengers wait in short or nonexistent lines for identity validation and screening. Technology standardization improve TSO effectiveness.	Data & Event Correlation, Identity Management, Incident Resolution, Standardization, Human Performance
Gate and Secure Area	Access to secure areas is restricted to individuals with valid credentials. Risk profiles, aggregate threat levels for flights, terminals, or airports.	Data & Event Correlation, Identity Management, Surveillance
Post Flight	Identity and risk profiles are anonymized for low-risk passengers to create data trends. Profiles for high-risk passengers feed future trips.	Identity Management

Where are we going?



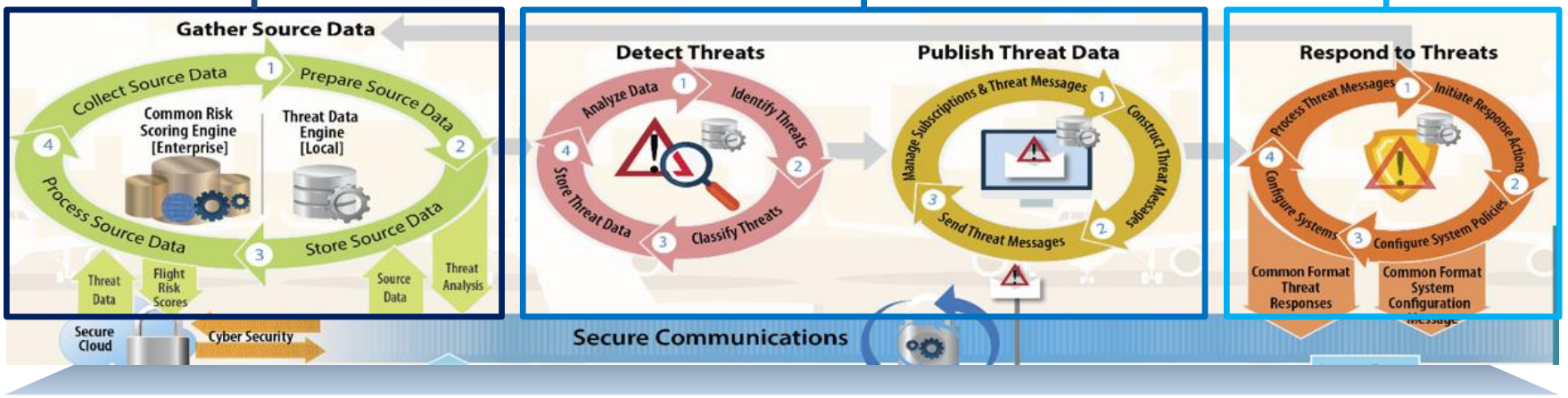
How does System Architecture change threat analysis?

The future state of 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.



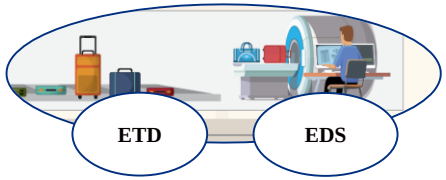
Real-Time Passenger Threat Information Sharing Between Security Screening Systems

Ticket purchase

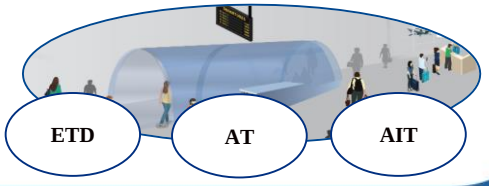
Check-in

Behavior Detection

Checked Baggage

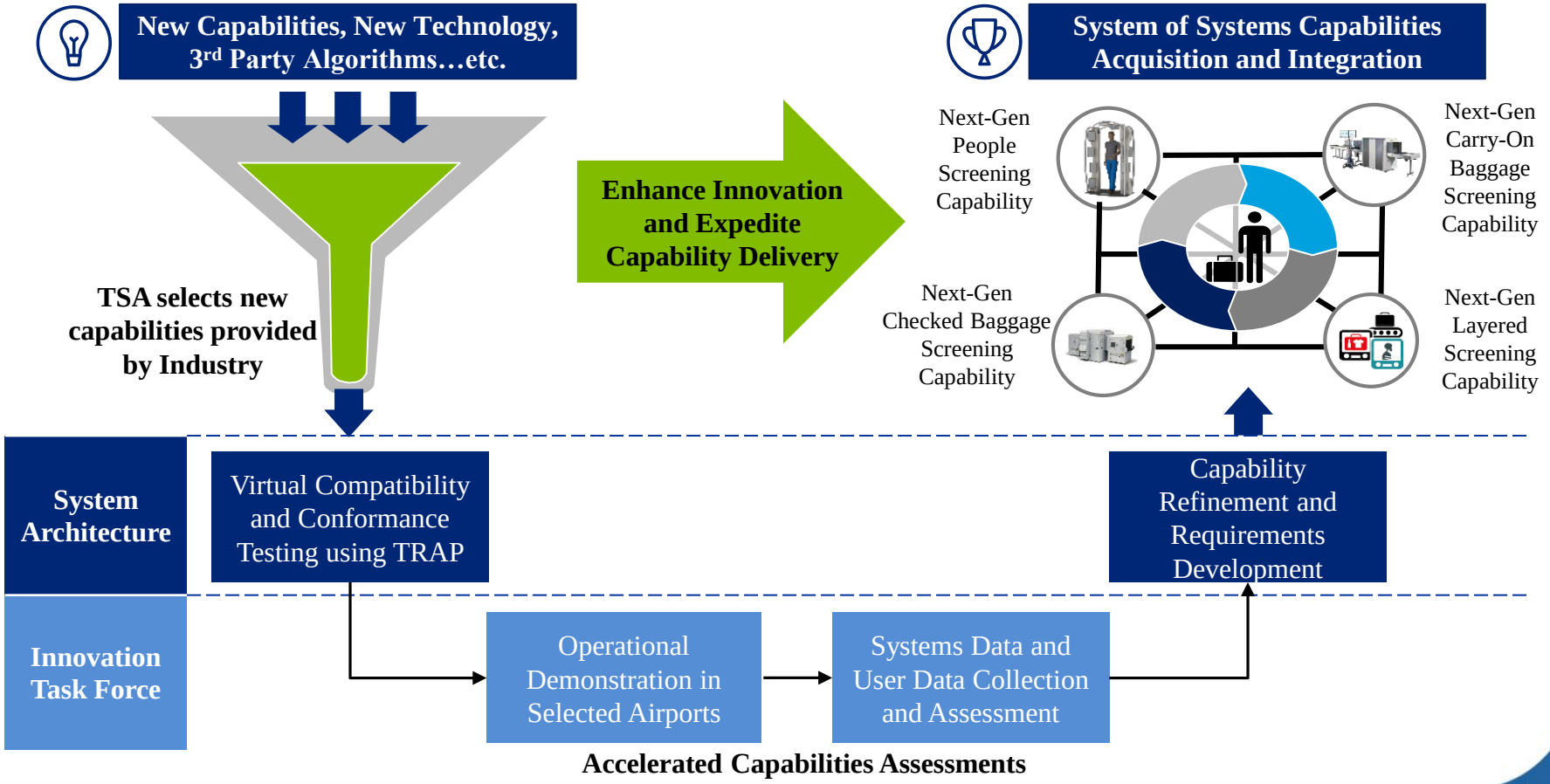


Checkpoint



How does System Architecture integrate with Innovation Task Force?

As the System Architecture team continues to define and develop a path to the system of systems security screening, integration with the Innovation Task Force (ITF) will further expedite the process of introducing new capabilities by demonstrating emerging solutions in the field and providing feedback to the System Architecture team for capability refinement and requirements development.

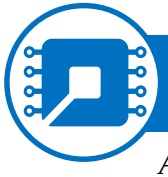


Appendix

- Alignment with Five-Year Plan
- OSC Leadership Prioritized Capabilities
- To-Be Architecture Overview
- TRAP Overview
- OTAP Overview

Alignment with Five-Year Plan

The following four themes were developed for the "Strategic Five-Year Technology Investment Plan for Aviation Security" and anchor our thinking towards developing an open OSC SA:



Enhancing Core Mission Delivery by Focusing on System of Systems

A push towards innovative concepts like interoperability and a system perspective will reduce complexity and help streamline requirements development, test & evaluation capabilities, and acquisitions

Streamlining Acquisitions, Requirements, and Test and Evaluation Processes

Focused investment on process improvement and business maturation activities throughout the acquisition lifecycle enables TSA to address dynamic, evolving threats posed to the nation's transportation network

Integrating Principles of Risk-Based Security in Capabilities, Processes, and Technologies

Comprehensive integration of risk-based security principles in mission capabilities enables security effectiveness throughout the screening process, cost and time efficiencies, passenger satisfaction

Increasing Transparency in Engagement with Stakeholders to Enable Innovation

Increased transparency with industry and DHS S&T stakeholders will result in enhanced collaboration, increasing the opportunities for businesses of all sizes to compete and help advance the mission of TSA

OSC Leadership Prioritized Capabilities

Security capabilities presented by participants have been grouped into ten capability categories and are listed in order of prioritization established during discussion.

1. Identity Management

Passengers are vetted at a high level so that verification is more accurate and risk levels are better understood in the aviation security system as a whole.

- Biometrics & Credentialing
- RBS
- Data Analytics

2. Integrated Network Architecture

An integrated network allows all TSEs and other technology devices to communicate seamlessly and supports data flow, allowing space for new capabilities and technology to be introduced.

- Dynamic Algorithms

3. Data and Event Correlation

Analytics and passenger data combined with real time events allow determination of an aggregate risk level for passengers / flights / airports.

- DARMS
- Predictive Forecasting

4. Contactless Screening

Measures taken to assess the threat of an attack from a distance allow for a more downplayed barrier to the secure area. Increased use of early, contactless screening improves security effectiveness while increasing throughput.

- Remote Screening
- Standoff Detection
- Vehicle Screening

5. Human Performance

Transportation Security Officers (TSOs) are more effective due to technology and process improvements.

- TSO Enablers
- Common GUI

Operational Efficiency: streamlining core processes and developing and implementing screening solutions

Passenger Experience: minimally invasive and unobtrusive screening that preserves privacy, dignity and can be intuitively regarded as necessary and thoughtful

Security Effectiveness: a measure of integrated, real-world performance insecurity screening according to a defined set of criteria designed to selectively identify and mitigate threats

OSC Leadership Prioritized Capabilities Continued

6. Incident Resolution

Incidents such as threats, attacks, surges in passengers, natural disasters or other events can be resolved or prevented through adaptive processes or technologies.

- Automated Incident Management
- Threat Resolution
- Surge Response

7. External and Partner Connectivity

As a result of coordination with Federal agencies, local authorities, and outside stakeholders, additional intelligence can supplement and enhance identity verification and risk/threat levels.

- Partnerships with CBP and across DHS
- Social Media Analysis

8. Surveillance

Surveillance methods allow aggregate data collection to feed risk profiles while tracking high risk passengers throughout the passenger journey.

- Video Analytics
- Automated / Remote Behavior Detection
- Undercover Agents

9. Physical Security

Ensuring the physical and cyber security for TSE and other equipment in the airport will enhance overall security awareness and vigilance.

- Access Control
- Physical Countermeasures (e.g. blast proof terminal fronts)

10. Technology/Process Standardization

Standard operations and technologies at airports ensure uniformity of experiences to enable quick introduction of new technologies while maintaining comparable detection standards across the aviation security system.

- Common Operating Platform
- Common Operating Procedures
- Traffic Management
- Queuing Analytics

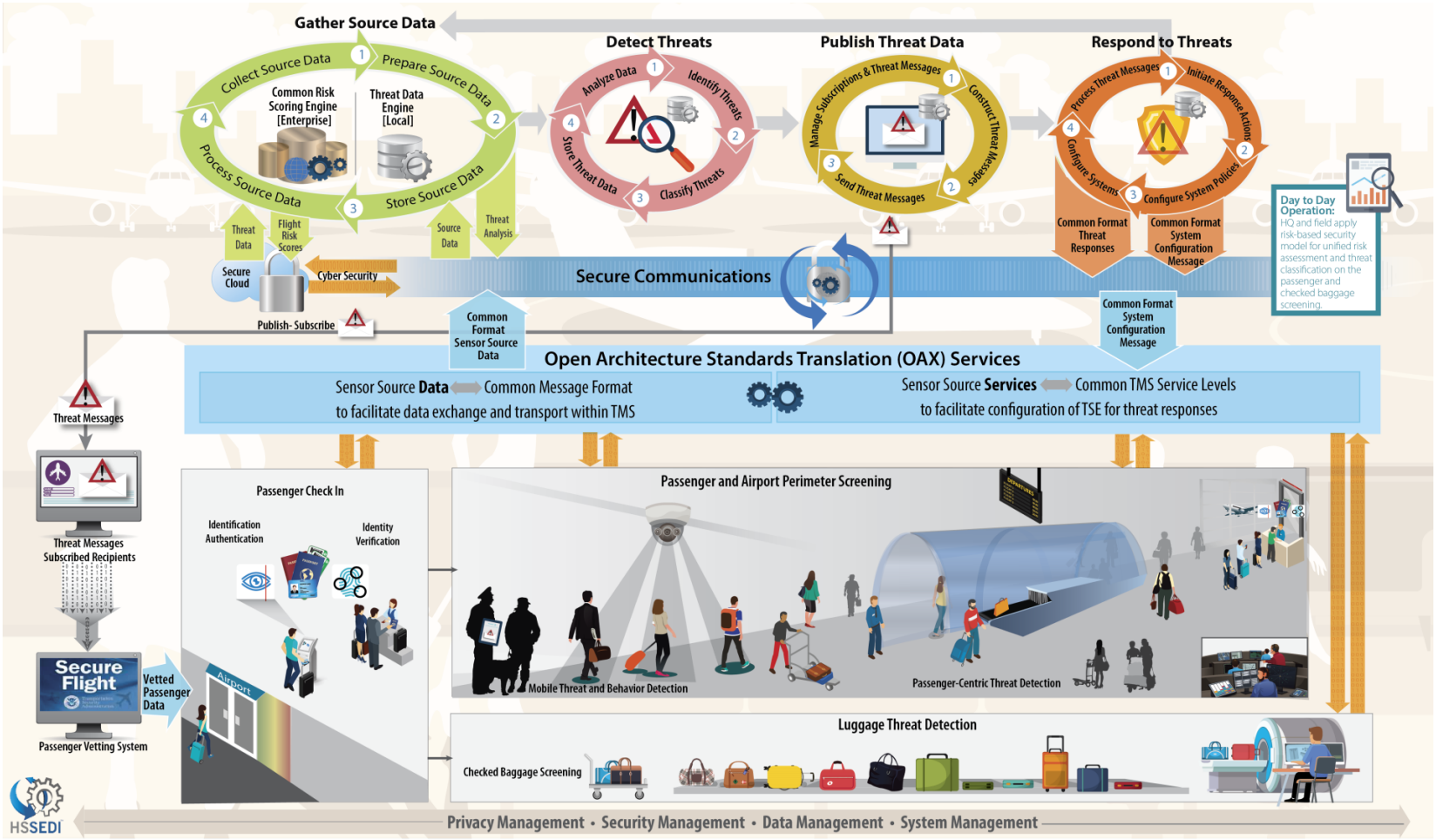
Operational Efficiency: streamlining core processes and developing and implementing screening solutions

Passenger Experience: minimally invasive and unobtrusive screening that preserves privacy, dignity and can be intuitively regarded as necessary and thoughtful

Security Effectiveness: a measure of integrated, real-world performance insecurity screening according to a defined set of criteria designed to selectively identify and mitigate threats

To-Be System Architecture

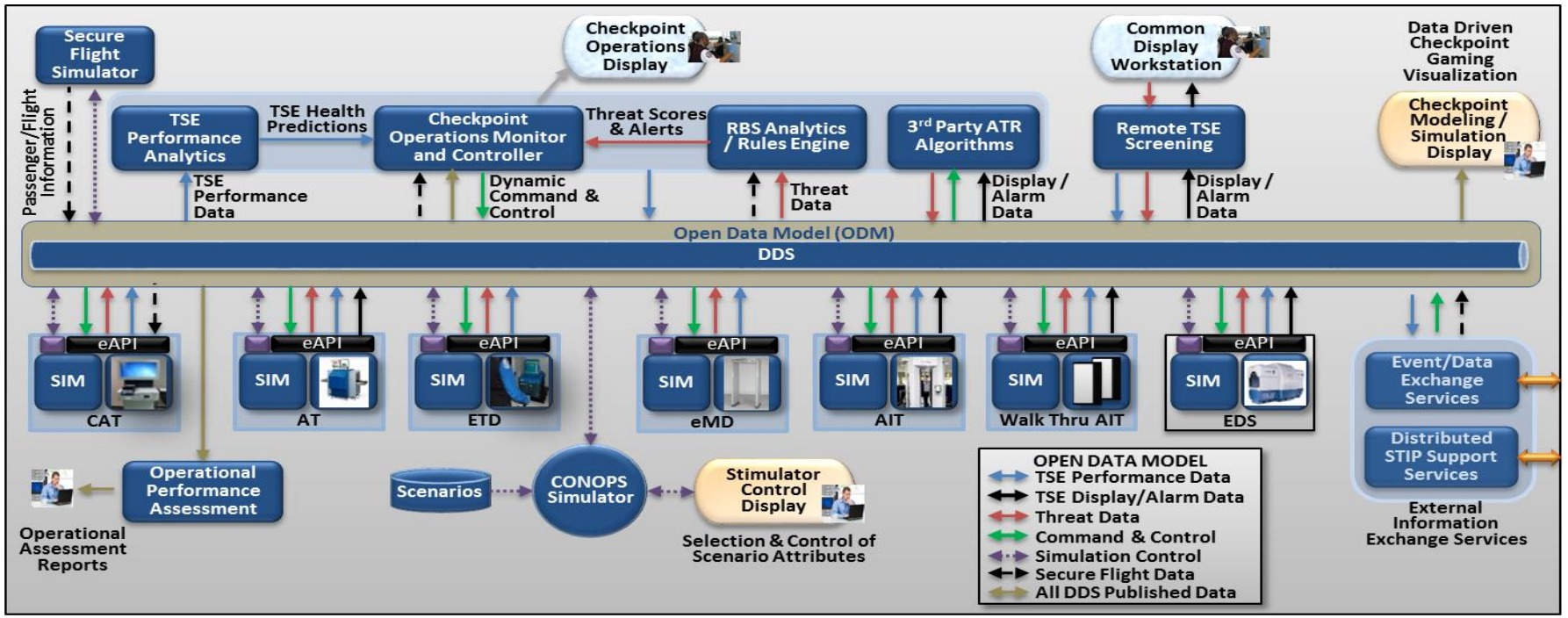
The "To-Be" system architecture outlines the future state of OSC System Architecture and will be used to inform TRAP development after validation.



TRAP Overview

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



OTAP Overview

OTAP will develop and demonstrate an open architecture baggage screening prototype in partnership with security technology manufacturers. This will allow for 3rd party vendors to implement detection algorithms and specialized hardware on screening technology.

Core OTAP Elements	
Open Platform Software Library (OPSL)	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.
Passenger Baggage Object Database (PBOD)	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.
Automatic Threat Recognition Algorithm *Integration*	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.
3rd Party Hardware Component *Integration*	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.
Human Factors Analysis of Data Visualization	Determine the types of data visualization and target detection algorithms that result in substantive enhancements to TSO target detection and collaborate with industry partners to develop and test algorithms along these lines.