SAND2016-0970C

Open Threat Assessment Platform

Industry Briefing

Mission Analysis Division

February 8, 2016

Transportation Security Administration

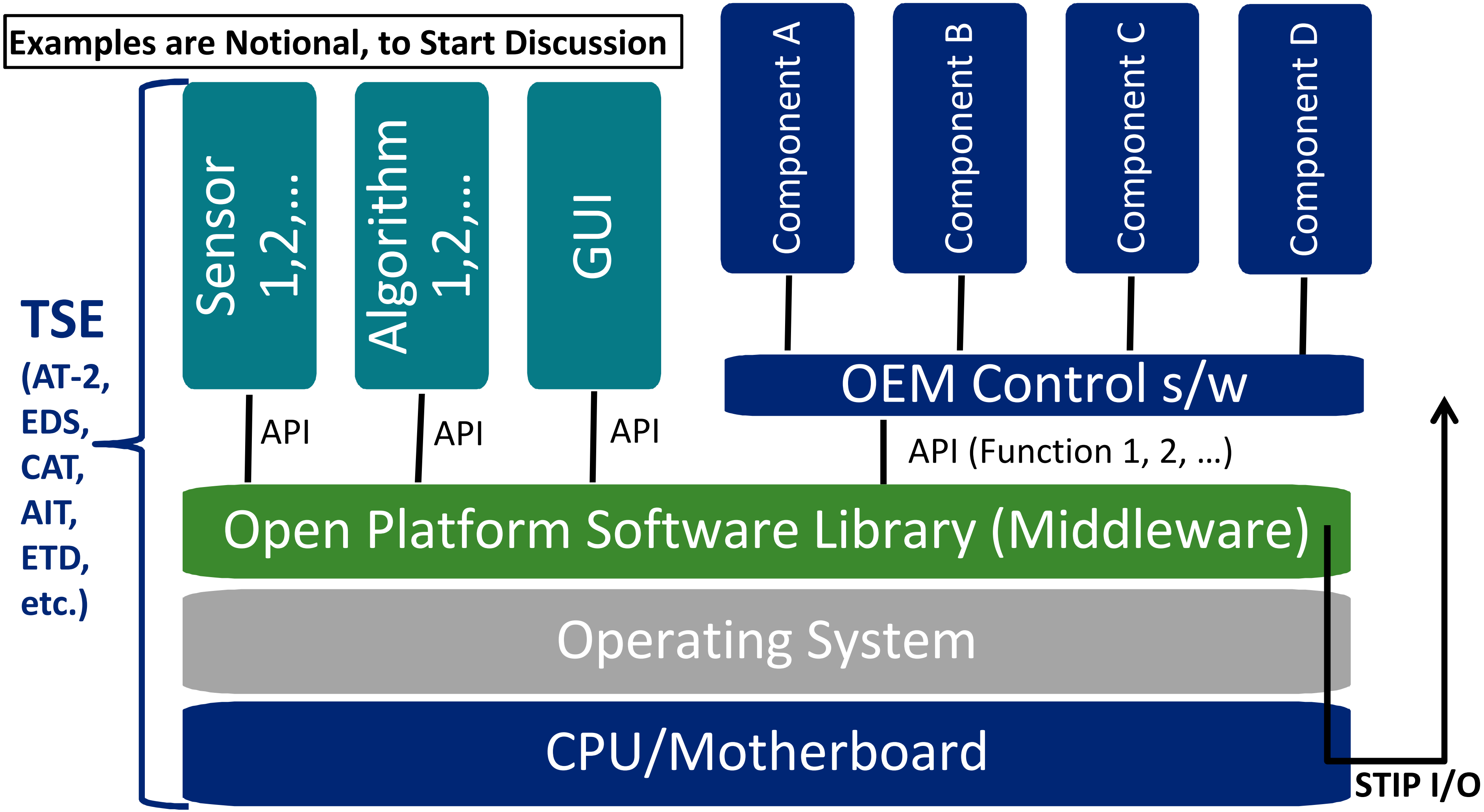
Preface

- The Open Threat Assessment Platform (OTAP) seeks to apply an open system architecture model to security *screening…focusing on equipment*.
- OTAP is a prototyping project and does not make or change TSA’s policy; but the OTAP experience and lessons-learned will inform policy.
- Industry has the expertise to develop fieldable, sustainable capabilities

OTAP’s Goal: Create an open architecture that enables *the broadest possible range of technologies and business models to flourish. A wider variety of vendors will more easily, quickly, and reliably be able to create capability upgrades (e.g. detection algorithms)* across the TSE fleet at lower cost to both vendors and TSA. The desired business outcome is to reward innovation and therefore sustain a healthier vendor market despite declining TSA budgets.

OTAP Middleware

Examples are Notional, to Start Discussion



🟦 OEM or 3rd Party | 🟦 OEM-Developed | 🟩 TSA-Developed

OTAP Project Strategy

Iterate to a working proof-of-concept deployed to an airport in order to work through the myriad, unpredictable technical issues associated with development *and* real-world operations.

Only a tangible proof-of-concept can provide TSA true confidence in the "implementability" of an open systems architecture (based on lessons learned from other technology deployments and attempts at system architectures).

1: Modular set of deliverables to hedge technical risk and still build foundations for a broader market.

2: Spiral development process with periodic deliverables prior to final. Adopt MVP concept.

3: Design for and integrate with TSA system architecture elements (e.g. STIP, DARMS).

4: Partner with private sector firms with specific expertise to harvest latest tech and ***ensure tech transition.***

5: ***Co-create new business model in collaboration w/TSA and industry*** to ensure viability of security technology market.

6: Attempt to future-proof the design; e.g. modularity, cyber-security, continuous diagnostics

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 (e.g., threat recognition algorithm for their seamless into a passenger baggage screening system. An open platform can be described as enabling a plug-and-play system not unlike third-party apps developed for smart-phones.

Passenger Baggage Object Database (PBOD)

- A database of X-ray-scanned outputs (e.g., raw radiography data, reconstructed images) of potential threats identified based on intelligence and analysis; information on non-threats; and any associated metadata that is used to train or build ATR capabilities. The purpose of PBOD is to contain in a single repository (or to make available to other authorized depositories) data that can be used to train algorithms for vetted vendors.

ATR Algorithm *Integration*

- A set of software applications that process the various signal outputs (e.g., both raw radiography data and image data) 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. 3rd party hardware components could be potential upgrades to existing screening equipment that may provide greater security performance.

RFQ Evaluation Summary

Sandia RFQ #577847, **X-ray Radiography Hardware System**, was issued on November 18, 2015 and closed on December 26, 2015.

Eight companies submitted responses to Sandia for this RFQ.

EDS / CT Systems

- 3 Companies

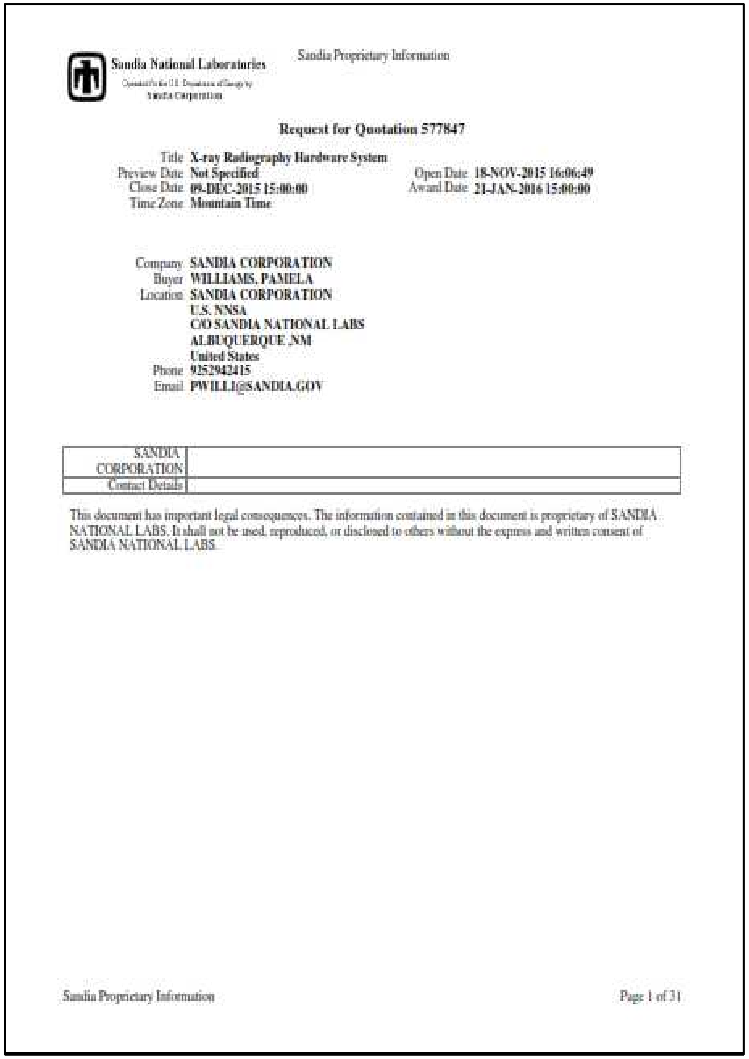
AT Systems

- 3 Companies

Data Acquisitions Systems

- 2 Companies

Awards expected in **February 2016**
Next two upcoming RFQs for software and hardware components



Sandia National Laboratories
Operated for the U.S. Department of Energy by
Sandia Corporation

Sandia Proprietary Information

Request for Quotation 577847

Title	**X-ray Radiography Hardware System**		
Preview Date	**Not Specified**	Open Date	**18-NOV-2015 16:06:49**
Close Date	**09-DEC-2015 15:00:00**	Award Date	**21-JAN-2016 15:00:00**
Time Zone	**Mountain Time**		

Company	**SANDIA CORPORATION**
Buyer	**WILLIAMS, PAMELA**
Location	**SANDIA CORPORATION** **U.S. NNSA** **C/O SANDIA NATIONAL LABS** **ALBUQUERQUE ,NM** **United States**
Phone	**9252942415**
Email	**PWILLI@SANDIA.GOV**

SANDIA CORPORATION	
Contact Details	

This document has important legal consequences. The information contained in this document is proprietary of SANDIA NATIONAL LABS. It shall not be used, reproduced, or disclosed to others without the express and written consent of SANDIA NATIONAL LABS.

Sandia Proprietary Information

Page 1 of 31

Internal & External Partnerships/Initiatives

Internal: OTAP platform leverages other initiatives, provides implementation path

STIP

OTAP uses STIP for TSE networking, will be STIP-compliant "out of the box"

DICOS

OTAP enables realization of these by providing middleware platform & by filling protocol gaps

TSE-SA & DARMS

Builds infrastructure that can support DARMS and overall architecture efforts

TRAP

Rapid eval. of new OTAP applications to more mature requirements

External: OTAP promotes mutual success by demonstrating OSC commitment

Hardware Partners

Access to TSE functionality and upgrade opportunities

Software Partners

Rapid development of cost-effective integrated software components

DHS S&T / APEX

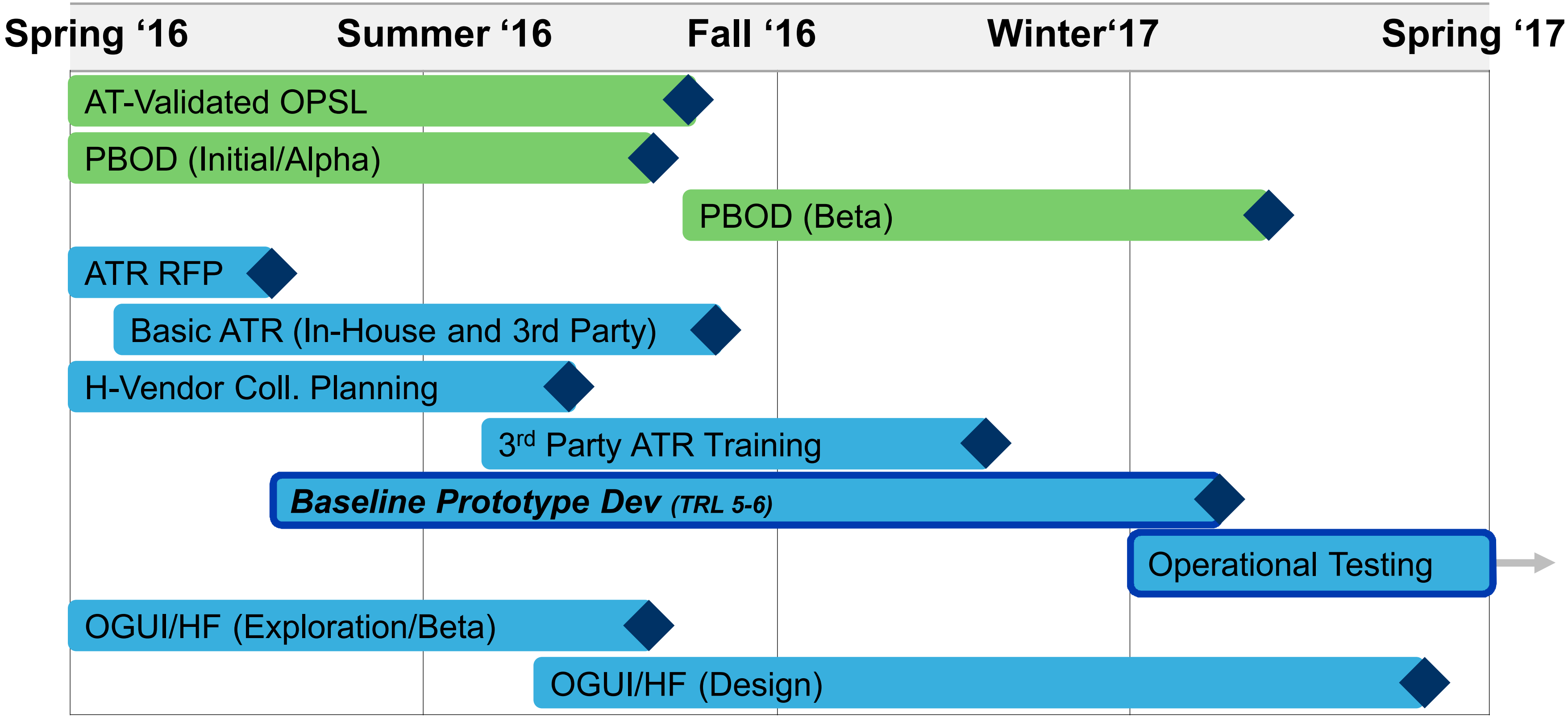
Benefits from better TSA rqmts via iterative / agile development, & by getting a platform for new sensors

SMC/Vendors

Helps vendors create predictable profitability
– AND –
Increases size of TSA market, and vendor access to it

Backup Slides

OTAP 18 Month Milestone Estimate



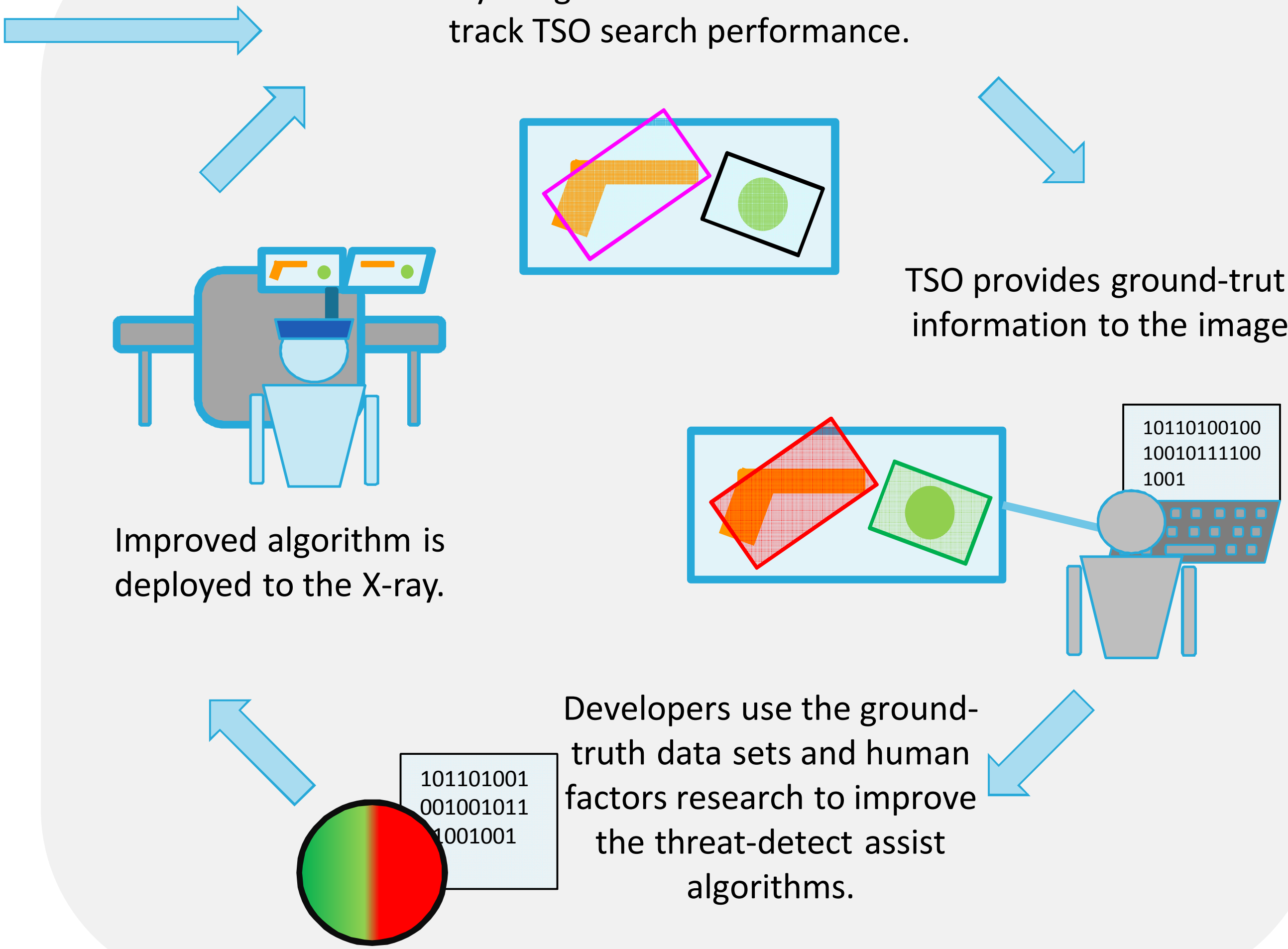
OPSL = Open Platform Software Library (aka middleware)
PBOD = Passenger Bag Object Database, for x-ray platforms (i.e. AT and EDS)

Prototype Concept

Develop API to a non-proprietary X-ray to decouple the hardware sensor and detection algorithm.

API

- Get_image()
- Get_data()
- Move_belt()
- Stop_belt()
- Annotate_image ()
- …



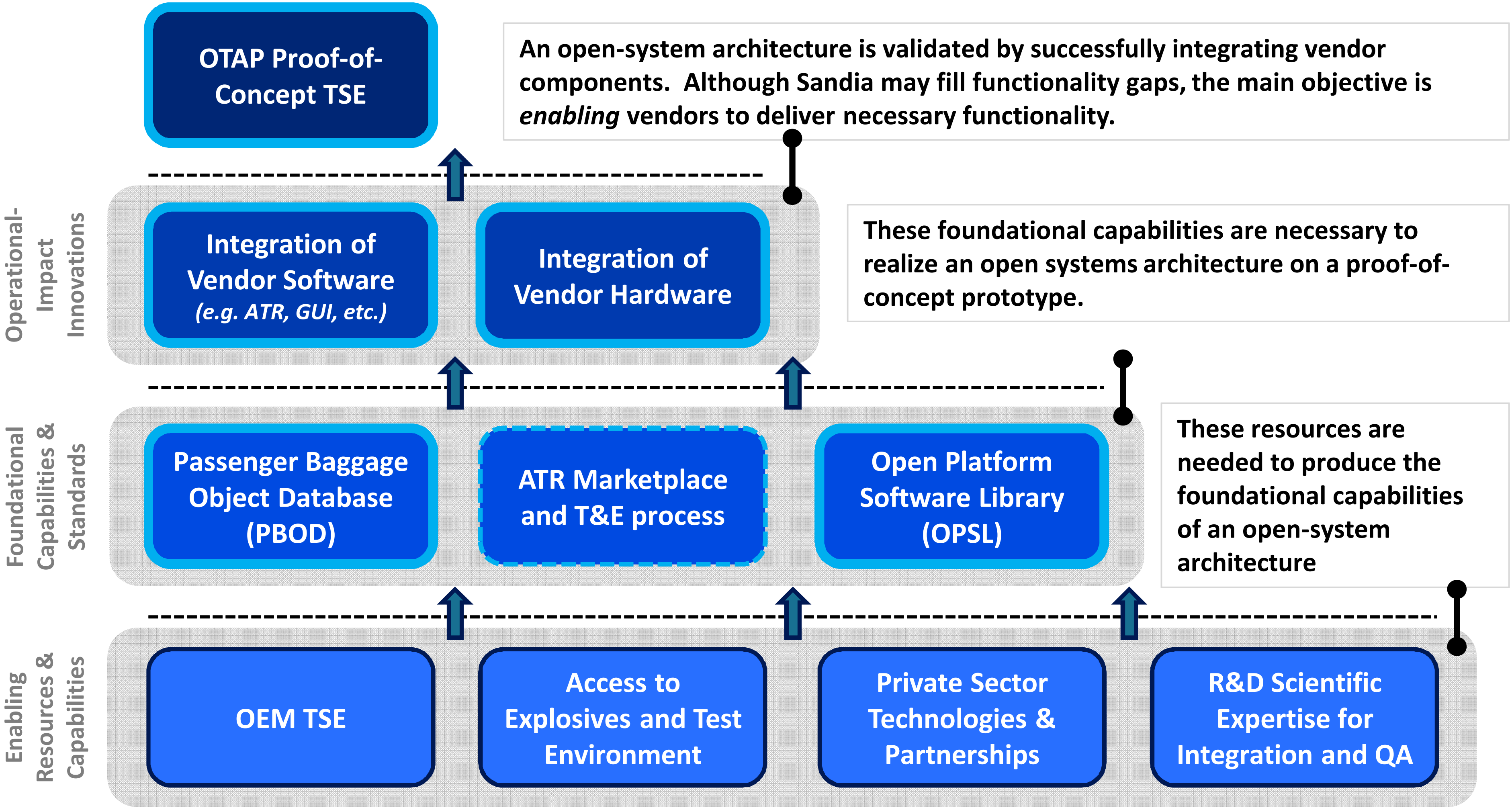
Detection algorithms annotate the X-ray image. Human factors metrics track TSO search performance.

TSO provides ground-truth information to the image.

Developers use the ground-truth data sets and human factors research to improve the threat-detect assist algorithms.

Improved algorithm is deployed to the X-ray.

OTAP Foundation



OTAP Proof-of-Concept TSE

An open-system architecture is validated by successfully integrating vendor components. Although Sandia may fill functionality gaps, the main objective is *enabling* vendors to deliver necessary functionality.

Operational-Impact Innovations

Integration of Vendor Software *(e.g. ATR, GUI, etc.)*

Integration of Vendor Hardware

These foundational capabilities are necessary to realize an open systems architecture on a proof-of-concept prototype.

Foundational Capabilities & Standards

Passenger Baggage Object Database (PBOD)

ATR Marketplace and T&E process

Open Platform Software Library (OPSL)

These resources are needed to produce the foundational capabilities of an open-system architecture

Enabling Resources & Capabilities

OEM TSE

Access to Explosives and Test Environment

Private Sector Technologies & Partnerships

R&D Scientific Expertise for Integration and QA

OTAP Goal: Build an open-system architecture that can a) successfully incorporate vendor capabilities, b) withstand the rigors of live operations, c) have a sustainable business model

OTAP Value Propositions

TSA

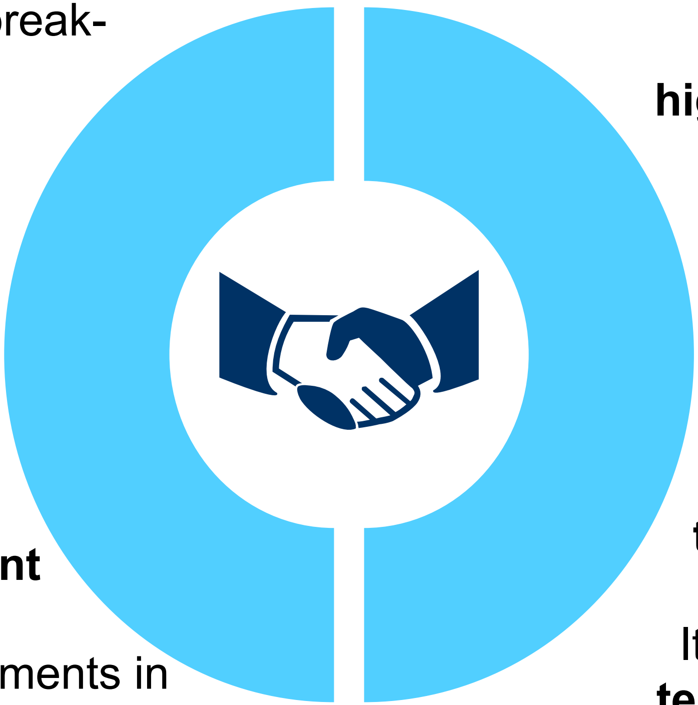
More capability advances, quicker to mature and at lower lifecycle cost

Analysis of best modular break-points helps define system architecture

Modular TSE interfaces **increases vendor access** to TSA market

Whatever Congress appropriates, TSA gets **more capability per $ spent**

Implements explicit commitments in **OSC Strategy, TSA 5-yr Tech Investment Plan,** & by **OMB/DHS**



Industry

More frequent, predictable and viable business opportunities with TSA

Modularity leads to **steadier high-margin revenue stream**

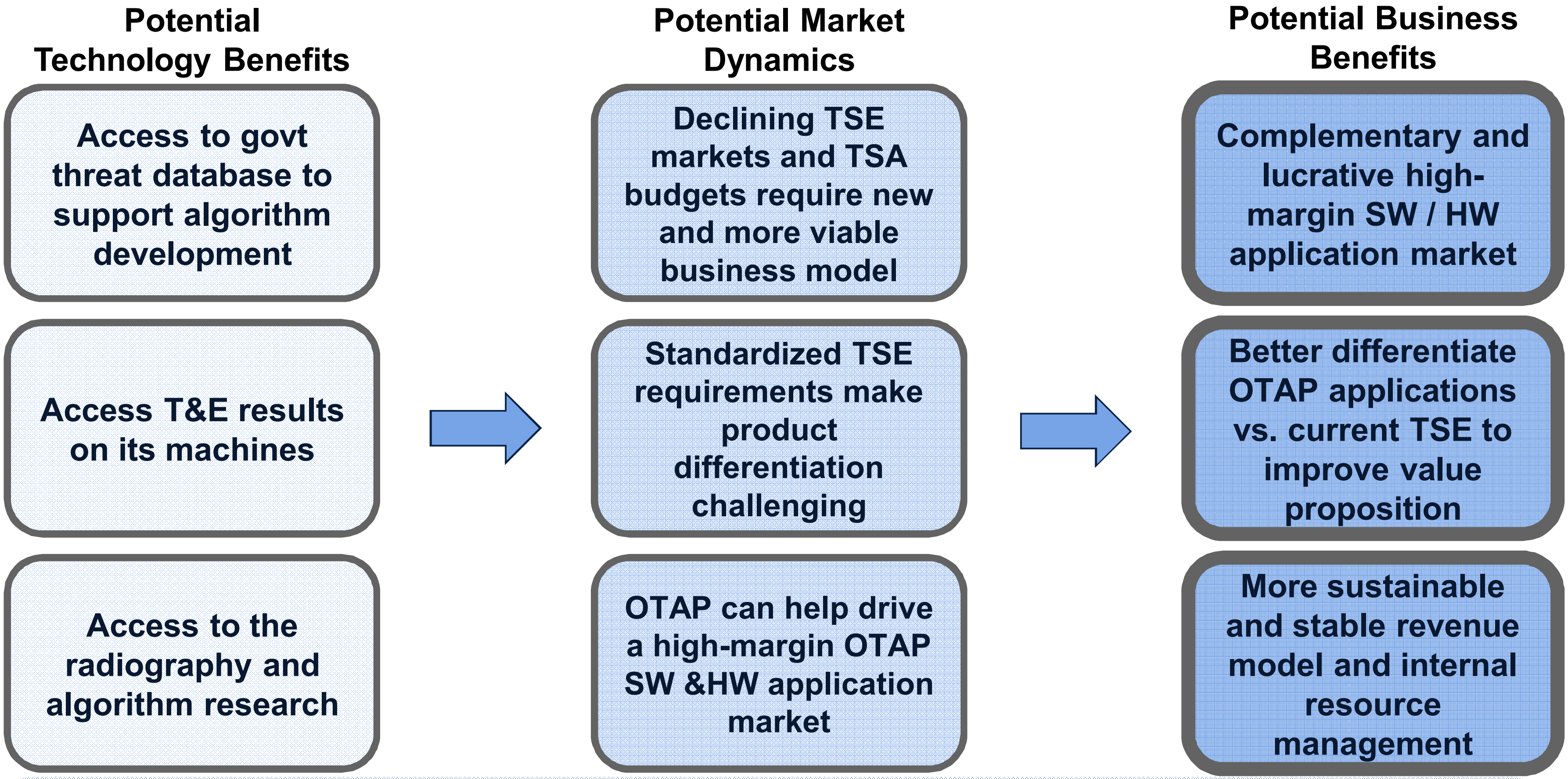
Access to **threat scan dataset** enables better, quicker sys. development

TSA-provided middleware & SDK **reduces barriers to entry** in TSA marketplace

Iterative prototyping **reduces technical risk, time and cost during T&E**

OTAP can create value for TSA and a more-vibrant security vendor industry

Value Chain for OEMs



Potential Technology Benefits

Access to govt threat database to support algorithm development

Access T&E results on its machines

Access to the radiography and algorithm research

Potential Market Dynamics

Declining TSE markets and TSA budgets require new and more viable business model

Standardized TSE requirements make product differentiation challenging

OTAP can help drive a high-margin OTAP SW &HW application market

Potential Business Benefits

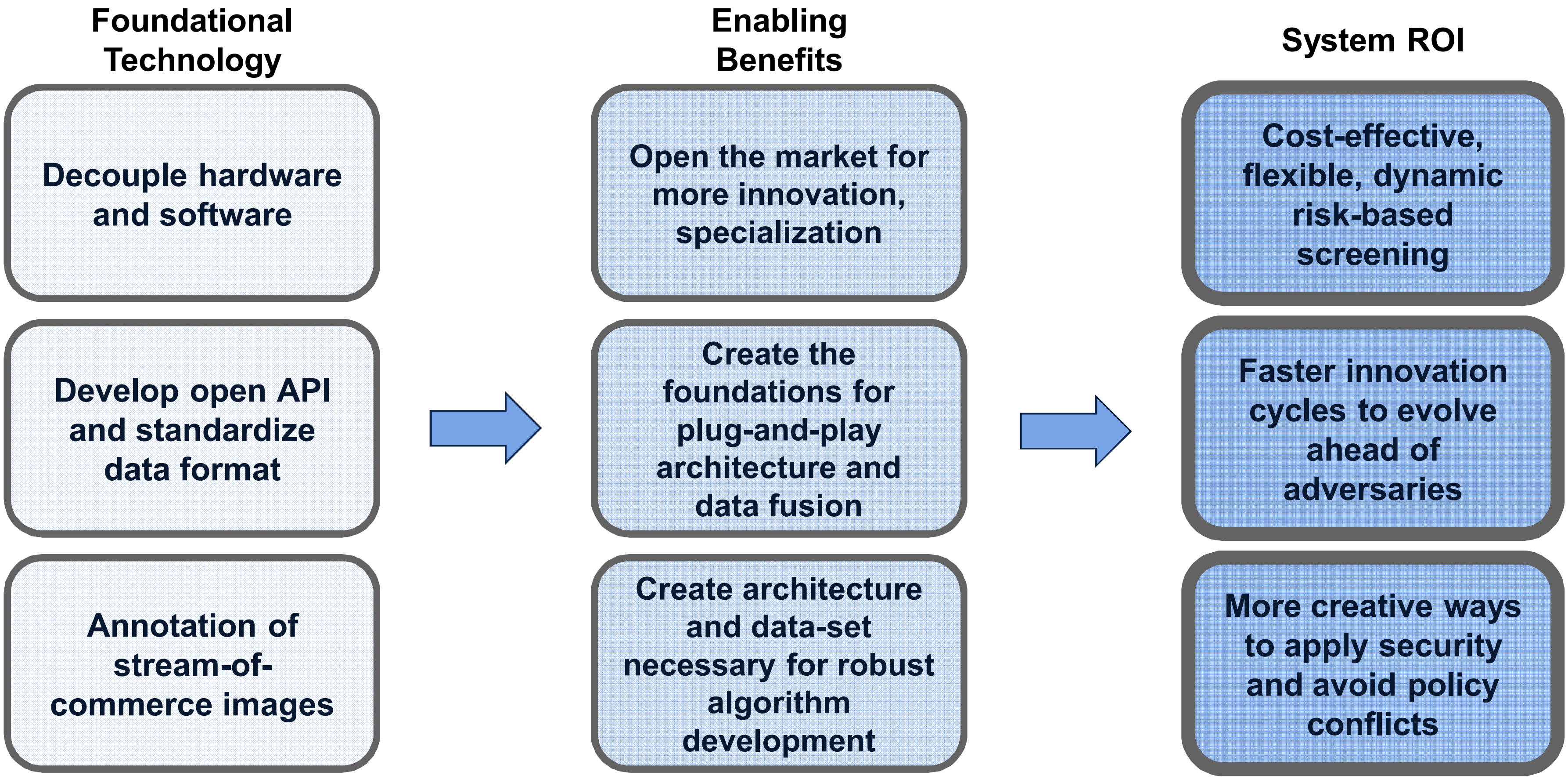
Complementary and lucrative high-margin SW / HW application market

Better differentiate OTAP applications vs. current TSE to improve value proposition

More sustainable and stable revenue model and internal resource management

TSE OEMs are well positioned and can be at the forefront of developing HW and SW upgrades and applications for the OTAP platform. **TSE OEMs can help shape the functionality of OTAP along with other vendors and jointly with TSA develop new and lucrative business models to better sustain their business.**

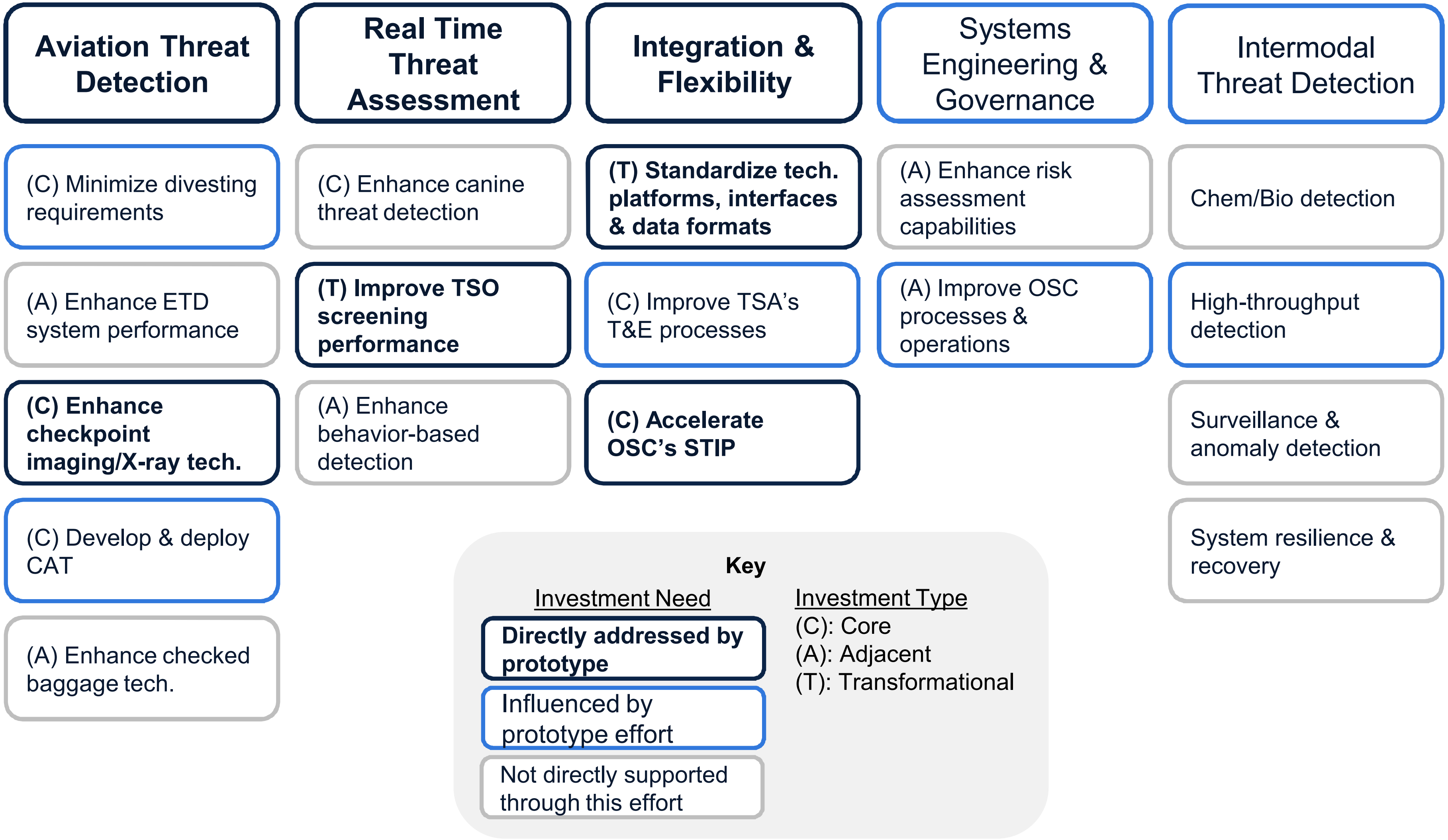
Value Chain for TSA



Foundational Technology	Enabling Benefits	System ROI
Decouple hardware and software	Open the market for more innovation, specialization	Cost-effective, flexible, dynamic risk-based screening
Develop open API and standardize data format	Create the foundations for plug-and-play architecture and data fusion	Faster innovation cycles to evolve ahead of adversaries
Annotation of stream-of-commerce images	Create architecture and data-set necessary for robust algorithm development	More creative ways to apply security and avoid policy conflicts

RBS vision requires foundational changes in technology and architecture to drive changes in the market and in how a screening system can be assembled. Once achieved, better security, efficiency, passenger experience, lifecycle costs, and industry vitality are possible.

TSA Capability Investment Plan



Aviation Threat Detection	**Real Time Threat Assessment**	**Integration & Flexibility**	Systems Engineering & Governance	Intermodal Threat Detection
(C) Minimize divesting requirements	(C) Enhance canine threat detection	**(T) Standardize tech. platforms, interfaces & data formats**	(A) Enhance risk assessment capabilities	Chem/Bio detection
(A) Enhance ETD system performance	**(T) Improve TSO screening performance**	(C) Improve TSA's T&E processes	(A) Improve OSC processes & operations	High-throughput detection
(C) Enhance checkpoint imaging/X-ray tech.	(A) Enhance behavior-based detection	**(C) Accelerate OSC's STIP**		Surveillance & anomaly detection
(C) Develop & deploy CAT				System resilience & recovery
(A) Enhance checked baggage tech.				

Key

Investment Need

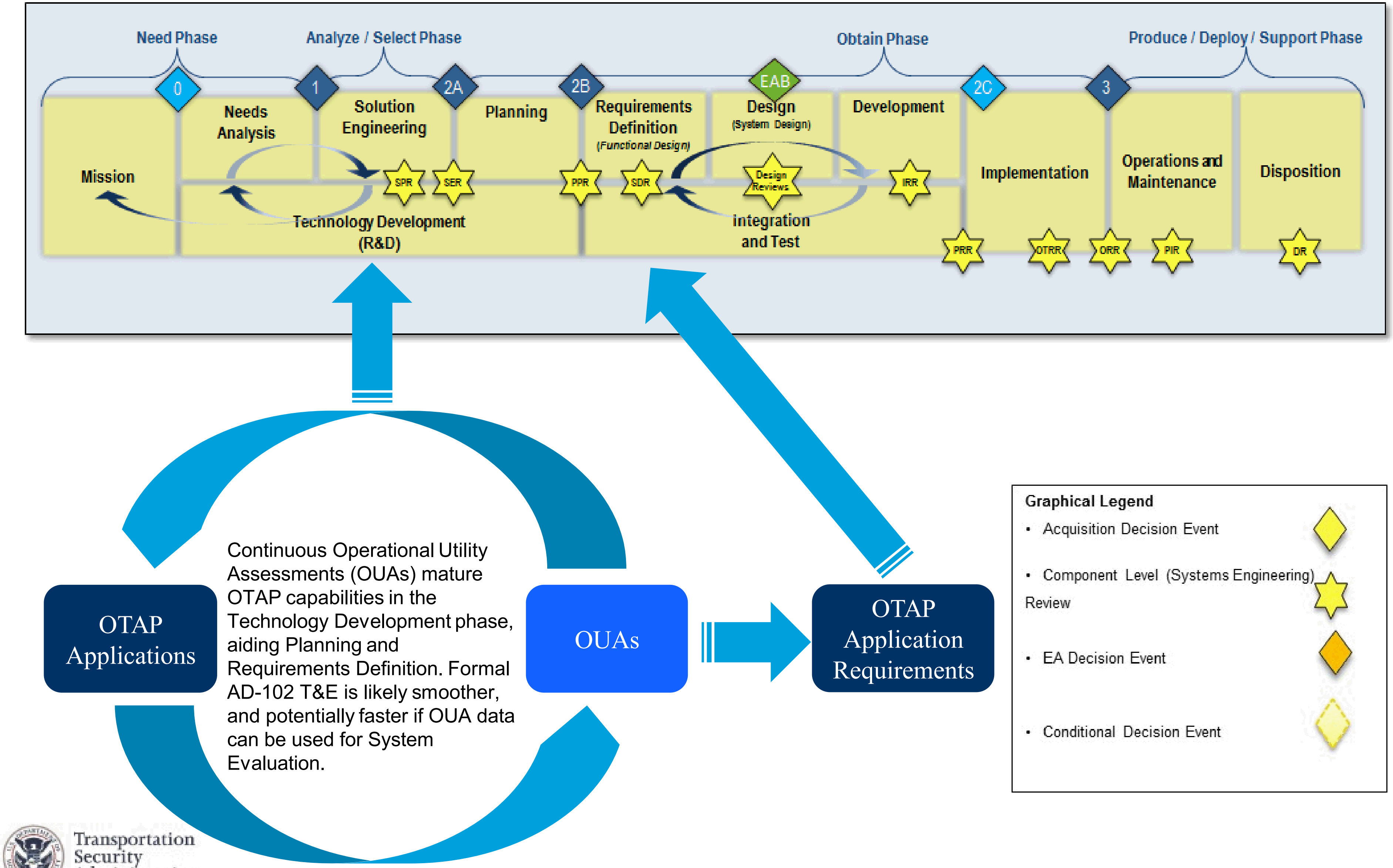
- **Directly addressed by prototype**
- Influenced by prototype effort
- Not directly supported through this effort

Investment Type

(C): Core
(A): Adjacent
(T): Transformational

Transportation
Security
Administration

DHS ALF and SELC (Golden Path)
(Proposed revision)



OTAP Applications

Continuous Operational Utility Assessments (OUAs) mature OTAP capabilities in the Technology Development phase, aiding Planning and Requirements Definition. Formal AD-102 T&E is likely smoother, and potentially faster if OUA data can be used for System Evaluation.

OUAs

OTAP Application Requirements

Graphical Legend

- Acquisition Decision Event
- Component Level (Systems Engineering) Review
- EA Decision Event
- Conditional Decision Event

Transportation Security Administration

Cybersecurity & Resilience Considerations

OTAP is being designed with security and resiliency as core principles. The OTAP team is assuming persistent hacking attempts.

Cyber Security Fundamentals

- Basics: e.g. no hardcoded password; separation of privileges; AV; etc.
- Compliance with relevant federal requirements (FIPS, NIST, DISA, TSA Handbook, etc.)

Secure Coding

- Open architecture / closed code → tight configuration control
- Architecture review
- Code reviews
- Static analysis
- Automated dynamic analysis
- Maybe: Formal Methods for Secure Coding

Cyber Red Teaming @ all phases of lifecycle

- Cyber security T&E prior to deployment of each version
- Regular/systemized penetration testing utilizing personnel with advanced skills
- Assessment across different OS’

Active Measures & Controls

- Failover architecture
- Runtime monitoring
- Infrastructure for rapid deployment of patches/updates

While no system can be 100% secure, secure coding practices, regular/systemized red-teaming, and active countermeasures can raise the difficulty of a cyber attack for adversaries.

Guiding OSC Principle: Open Systems Architecture

"Underpinning this challenge [lack of dynamic threat detection] is the fact that **current systems are highly complex and proprietary with little data, image or interface standardization**. This means that OSC must depend solely on the equipment manufacturer and existing contracting mechanisms for software, algorithm, component or operational upgrades. This limitation prevents OSC from engaging new and innovative partners to solve problems and can slow response to the emerging needs." –*TSA Capability Investment Plan (2014)*

"We need to move to an open systems architecture" –*Jill Vaughn , OSC AA (2015)*