Checked Baggage Capability Maturation Roadmap

September 2023

Table of Contents

Administrator's Message

September 2023

Since its inception, the Transportation Security Administration (TSA) has been dedicated to protecting the nation's transportation systems to ensure freedom of movement for people and commerce. Checked Baggage Capability Management (CBCM) is critical to TSA's mission because it ensures the safety of the traveling public on all commercial flights, both domestic and internationally. The CBCM Roadmap builds on existing checked baggage screening technologies as well as emerging solutions that increase security effectiveness and efficiency. This Roadmap will serve as the blueprint for future CBCM work across the agency, and addendums will be published to expand on impending priority topics.

As we explore solutions to meet the goals and objectives identified in this Roadmap, it is important that we think toward the future. Open Architecture is a key capability that is needed for checked baggage development. Open Architecture will enable various initiatives, including One Stop Security (OSS) for trusted international partners and regionalized On-Screen Alarm Resolution Protocol (OSARP) within the domestic U.S. Open Architecture will also simplify the procurement process for Explosive Detection Systems (EDS) enhancements and support the possibility for third party advanced algorithm development.

TSA must also bolster its cybersecurity requirements and Information Technology (IT) infrastructure in order for Open Architecture to become a reality. Other technologies, such as X-ray Diffraction (XRD), Differential Phase Contrast (DPC), Artificial Intelligence (AI), and Machine Learning (ML) also present new possibilities to improve checked baggage screening while mitigating risks to our transportation systems. TSA is committed to protecting the transportation sector as new threats continue to evolve.

I want to thank everyone at TSA and our industry and interagency partners who had a hand in creating this Roadmap, as well as all those who work to achieve its goals each day. Together, we will make its vision a reality and continue to achieve to the high expectations of the traveling public, our stakeholders, and each other.

David P. Pekoske
Administrator

Introduction

The Transportation Security Administration's (TSA) Requirements and Capabilities Analysis (RCA) office determines the strategy and development of TSA's security architecture and operational capabilities to enhance security and optimize performance. This is integral to achieving TSA's mission of securing the transportation systems while ensuring freedom of movement for people and commerce. TSA's Acquisition Program Management (APM) office is responsible for delivering innovative, mission-driven capabilities required by the frontline to safeguard America's transportation systems. To this end, both APM and RCA collaboratively manage the Checked Baggage[1] mission space through the Electronic Baggage Screening Program (EBSP) and the Checked Baggage Capability Manager (CM) Teams respectively.

The APM Program Management Office (PMO) manages EBSP in compliance with Department of Homeland Security (DHS) and TSA acquisition policy and is responsible for identifying, testing, procuring, deploying, installing, sustaining, and recapitalizing Transportation Security Equipment (TSE) across all federalized airports to ensure 100% screening of Checked Baggage. RCA's Checked Baggage CM focuses on Research & Development (R&D) associated with future EBSP capabilities, identifying operational improvements, and maintaining the Standard Operating Procedure (SOP) for the field to ensure clear and consistent instruction.

As such, TSA is responsible for the security screening of Checked Baggage from the moment the property is presented for screening until screening has been completed and cleared for transport onboard the aircraft.

As threats to our mission space continue to evolve, so must TSA's technology and mitigation strategies to ensure mission success. If an adversary is able to exploit security vulnerabilities in the global security infrastructure, the potential for harm to the traveling public increases exponentially, as gaps could be exploited in any airport nationwide and globally. To mitigate evolving threats and capability gaps in the checked baggage environment, RCA and APM are dedicated to guiding the maturation of the Checked Baggage Capability across the TSA Enterprise.

The primary objective for Checked Baggage stakeholders is to develop, acquire, and implement dynamic material and non-material based, modular capabilities that will enhance TSA's ability to improve aviation security while enhancing the experience of the users of the technology and capabilities, Transportation Security Officers (TSOs). As part of this objective, TSA sees Open Architecture as a means to support rapid development of capability, expand engagement with industry, and promote an overall improved Checked Baggage system-of-systems.

To guide the developmental progression of the Checked Baggage Capability, RCA and APM have developed a strategic Roadmap outlining capability enhancements and technology upgrades over the next several years. This Roadmap outlines TSA's current state and future vision for the Checked Baggage Capability and is designed to guide TSA's long-term research, development, procedures, and acquisition strategy for Checked

1 Checked Baggage includes property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during the flight. Accompanied commercial courier consignments are not classified as Checked Baggage, and undergo screening in compliance with the cargo screening requirements.

Baggage as it matures. Ultimately, the matured state is characterized by an increased ability to detect an expanded set of threat materials at higher detection rates, lower false-alarm rates, and lower lifecycle costs. Ideally, all future enhancements and capabilities will improve the operator experience by reducing the cognitive burden on TSOs. All activities described are either directed toward enabling technologies and processes or improving existing capabilities to enhance Checked Baggage screening capabilities.

One of the major sources of appropriation for these activities is the Aviation Security Capital Fund (ASCF), which Congress established in 2004. Under this appropriation, APM receives $250 million annually to support TSA's compliance with the 100% checked baggage screening mandate. The funds also allow TSA to test, procure, install, sustain, and recapitalize Explosive Detection Systems (EDS) and Explosive Trace Detection (ETD) to support checked baggage operations across all federalized airports. ASCF supports capital projects that reduce risk and increase security effectiveness and screening efficiency through the design and implementation of new inline EDS systems and the recapitalization of inline EDS systems. Finally, ASCF supports the procurement and installation of enhanced functionalities/capabilities (detection, cybersecurity, user interface, etc). ASCF is not authorized to support R&D activities.

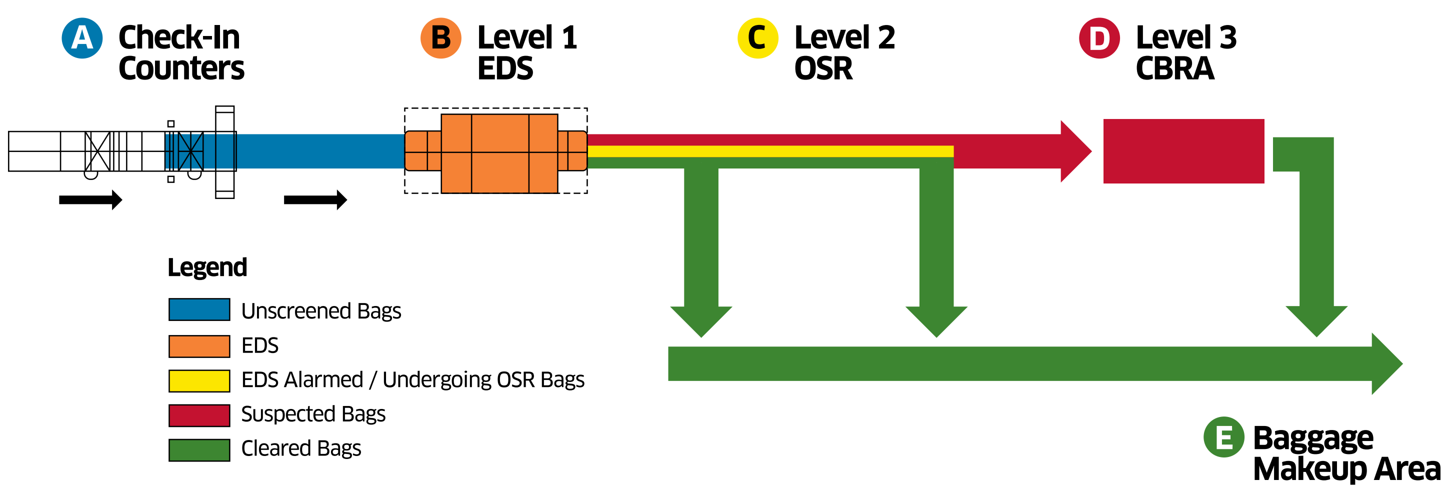
If the ASCF appropriation is extended to support the next checked baggage program of record, ASCF would continue to support the testing, procuring, and installation of checked baggage technologies based upon a system of systems methodology that supports the principles of Open Architecture.


TSA
TSA
32-12

Current State of Checked Baggage Screening

Prior to COVID-19, TSA screened approximately 1.4 million checked bags per day for explosive materials. The use of explosives within Checked Baggage remains an attractive target for threat actors to exploit. To mitigate the risk of using Checked Baggage as a threat vector, TSA employs two major technologies, in varying configurations, to detect explosive threats. The technologies include the explosives detection system (EDS) and explosives trace detection (ETD), which rely on computed tomography (CT) and ion mobility spectrometry technology respectively. The Checked Baggage fleet consists of approximately 1,689 EDS units and 2,638 ETD devices. Checked Baggage screening involves three different screening levels:

- **Level 1** screening is performed with EDS units at most airports but can also be performed with ETDs. All bags that can physically fit within the aperture of an EDS unit are directed through Level 1 screening. All bags that automatically alarm at Level 1 are subject to Level 2 screening.
- During **Level 2** screening, TSOs view alarmed images captured during the Level 1 EDS scan, and clear alarms that can be resolved visually through On-Screen Alarm Resolution Protocol (OSARP). All bags that cannot be resolved at Level 2, and all bags that cannot be directed to Level 1 due to size restrictions, are sent to Level 3 screening.
- **Level 3** screening is performed manually and involves physically opening the bag and the use of ETD technology. The bags that are not cleared by a TSO at Level 3 are referred to Transportation Security Specialists-Explosives (TSSEs) or local law enforcement to make a final determination as to the disposition of the bag.



TSA has deployed an advanced fleet of Checked Baggage screening equipment to meet the security needs of the nation's aviation system. TSA continues to work with industry to apply spiral and incremental approaches to technology development. This allows TSA to procure technologies and upgrade existing machines as new capabilities arise, instead of requiring complete system recapitalizations. Additionally, TSA has developed a test kit to validate the performance of currently fielded EDS. The test kit is currently in use for Site Acceptance Tests (SAT).

TSA deploys EDS machines with varying levels of integration, such as in-line and stand-alone configuration. The in-line configuration referred to as Type 1, matrixes multiple EDS via a closed network and integrates them with an airport's baggage handling system (BHS) – the conveyor system that sorts and transports baggage for loading onto an aircraft. The infrastructure of equipment is known as the Checked Baggage Inspection System (CBIS) and its various components are managed by the airport authority, airline, and TSA. EDS in stand-alone configurations are referred to as Type 2 and are individual baggage screening units that are not matrixed nor are the majority integrated with a BHS. The Type 2 systems are typically located in an airport lobby or in other airport locations such as oversized baggage acceptance areas.

Checked Baggage Capability Maturation Roadmap

After assessing the current state of Checked Baggage, RCA and APM created this Roadmap to outline a multi-phased approach to mature the Checked Baggage Capability in distinct phases. The Checked Baggage Roadmap is divided into three functional areas, **Detect**, **Connect**, and **Enable**, each with their own subcategories. The Roadmap defines the envisioned future state of the Checked Baggage Capability and incremental milestone development within each functional area.

Detect **Connect** **Enable**

Future efforts in research and development identified in the Roadmap will focus on the following:

- EDS Enhancements
- Advanced Algorithm Deployment
- Stream of Commerce False-Alarm Reduction
- Open Architecture
- Threat Characterization
- Data Mining
- Remote Screening
- System Analysis and Modeling
- Cybersecurity

Detect

The first identified function of the Checked Baggage Capability refers to employing technology to determine if threats are present in checked baggage, ensuring the highest probability of detection with the lowest probability of false alarm, while maintaining baggage throughput.

EDS Machines

RCA and APM are working in collaboration to develop operational and functional requirements for next generation EDS machines. These requirements will help improve EDS detection of explosives to include the ever-evolving threat of homemade explosives. The commercial development of these next generation systems will help enhance security effectiveness. Work is ongoing to develop a Concept of Operations (CONOPS) to utilize designated test kits to determine and asses EDS performance and degradation over time. This CONOPS will support confirmation of detection performance.

Detection Requirements

TSA develops detection requirements for screening technologies. These detection requirements leverage multiple information streams such as intelligence reporting, adversarial threat preference, aircraft vulnerability testing, threat prioritization, risk analyses, and performance trade space (detection vs. false alarm performance). The detection requirements are updated periodically to account for emerging threats identified through sources such as intelligence reporting and risk analyses. Currently, detection algorithms are developed by the Original Equipment Manufacturers (OEMs) and used exclusively with that OEM's proprietary equipment. TSA is working closely with OEMs to develop and deploy improved detection algorithms on in-service EDS units.

The PMO is also streamlining acquisition processes by developing and implementing Detection Functional Requirements Documents (DFRD) from Detection Requirements which enable incremental performance improvements and improve the time to field enhanced capabilities. Also, DFRDs afford an opportunity for RCA and APM to perform trades in probability of detection (Pd) and probability of false alarm (Pfa) so as to deploy enhanced detection capability without breaching baseline field false alarm rates. The implementation of new threat detection algorithms on new and existing TSE is expected to improve TSA's ability to detect a wider range of threats while decreasing the probability of false alarms.

TSA is exploring technologies capable of distinguishing between concealed threats and Stream of Commerce (SOC) items. Currently, EDS systems are X-ray based and use effective atomic number and density to discriminate between objects. TSA needs to detect new types of threats in smaller masses while also accommodating for growing traffic volumes. TSA needs to move away from proprietary algorithms and begin utilizing Open Architecture concepts such as common data formats and standardized interfaces. This change will facilitate faster, universal solutions to the field while providing cost savings to the agency by procuring each algorithm only once.

Additionally, the introduction of new technologies, such as X-ray Diffraction (XRD) and Differential Phase Contrast (DPC) to legacy algorithm approaches provides the potential for enrichment of detection probabilities across the span of current and emerging threats. To improve material recognition and threat identification, industry and academia have created experimental test beds to accelerate testing, development and deployment to the field. By improving material discrimination, it will increase the ability to detect currently unidentifiable threats and differentiate between threat and non-threat materials.

False Alarm

To reduce the probability of false alarms, TSA is exploring new detection algorithms and other detection methodologies such as XRD and DPC to improve system efficiencies and enhance material discernment. These applications may be an additional step in the screening process, may usurp traditional screening technologies, or be layered in parallel on the existing screening process. Data mining is needed to better understand the SOC causing the false alarm to support these solutions. TSA has also incorporated reduced false alarm requirements in the detection requirements previously outlined.

The purpose of these requirements is to achieve optimal operational efficiency by minimizing operator complexity in threat adjudication, optimizing TSO utilization rates, integrating into the TSA enterprise using a sound cybersecurity approach, and allowing system updates with new algorithms for emerging threats. Leveraging Open Architecture to capture and share SOC data will further support continuous improvements to detection algorithms to drive down false alarm rates.

Connect

The second identified function of the Checked Baggage Capability refers to leveraging Information Technology (IT) systems to allow for Near Real-Time (NRT) data capture and storage at the enterprise level and distribution at the checkpoint to enable risk-based dynamic screening concepts. As such, NRT data capture can enable and empower data-driven decision making at TSA to inform and optimize the allocation of airport resources. The future state of this capability is to enable secure and remote data transmission to derive meaningful and data-driven insights in NRT as well as operationalize threat assessments.

To do this, the Checked Baggage Capability will comply with the Federal Information Security Management Act (FISMA) as the PMO will establish and maintain an Authority to Operate (ATO) to ensure cybersecurity controls for Checked Baggage security systems. Connectivity will enable TSA to pursue additional capabilities such as the use of Artificial Intelligence and Machine Learning (AI/ML) to screen checked baggage, the automated switching of detection algorithms, and route bags of known or suspected terrorists to additional screening in real time.

Data Mining

Data mining involves the use of data analysis tools to discover previously unknown, valid patterns, and relationships in large data sets. Data mining captures data through the screening process and applies it as inputs to machine/deep learning-based algorithms. Additional benefits of data mining include reducing the false alarm rate and cognitive load on TSOs. Overall, data mining can optimize the allocation of airport resources such as staffing.

Cybersecurity

The TSA Information Assurance Cybersecurity Division (IAD) will define the requirements for an ATO of a connected Checked Baggage information system. These requirements will be necessary to define data types, data storage, physical security, user access and control, operating system (OS) hardening, audit and logging, virus protection and patch management, user needs, Personal Identity Verification (PIV) based authentication, security event monitoring, and vulnerability scanning. IAD will follow the FISMA 2014 U.S. Federal Law using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Special Publication (SP) 800.53 Rev. 4 Information Assurance (IA) Controls, DHS policies, TSA polices, and the Department of Defense (DoD) Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

Network connectivity to the TSA IT Enterprise network is a prerequisite before establishing and enabling these capabilities and will support the capabilities to be enabled within the system (for example, algorithm switching). Checked Baggage intends to use network connectivity to securely exchange data between Transportation Security Equipment (TSE), the enterprise, and external databases. Additionally, network connectivity will ensure the ability to push operating and detection software updates and perform remote maintenance and monitoring over the network, rather than requiring in-person visits from field technicians.

Through remote monitoring and maintenance, TSA can be more readily notified of performance issues or risks to systems in the field. Furthermore, network connectivity will allow the Command and Control of interconnected machines to respond quickly to emerging threats by deploying real-time algorithm upgrades from TSA headquarters to the field. Future capabilities will require that EDS platforms comply with the requirements of the ATO which are derived from the NIST RMF SP 800.53 required security controls for moderate categorized systems, plus overlay the controls required for mission essential systems and high value asset systems.

For technologies to be allowed to connect, Security Technology Integrated Program (STIP) enabled operating systems will be required to include OS-based, TSA approved encryption for both the hard drive and ransomware backup and/or protections. Systems will also be required to meet U.S. supply chain requirements for vendors, possess enough memory and hard drive space to allow software installation setups, sustainment, and antivirus protection, and be capable of supporting frequent software (OS and application) cybersecurity patches as well as monthly and ad-hoc Nessus scans. Physical access controls will also need to be governed tightly, and all open ports must have locked covers/protectors or be protected inside housing and/or coverings when not in use. Routine maintenance of these devices at airports must only be allowed with TSA issued and approved USB devices and/or computers/laptops.

Systems that are unable to achieve these requirements will not be allowed to connect and are not viable technologies for the operational environment.

Remote Screening

TSA is interested in exploring international to domestic remote screening through Open Architecture based systems. Currently, inbound international travelers who are continuing onto other domestic locations enter at a U.S. international airport are cleared by U.S. Customs and Border Protection (CBP). Passengers must collect their checked baggage and proceed through the entry process. Once the traveler completes the Customs inspection process, the traveler must then recheck baggage for onward travel.

To expedite this process, DHS Science and Technology (S&T), CBP, and TSA are exploring a series of proof of concepts with trusted foreign governments and industry partners that will help determine the feasibility of virtually screening baggage and thus eliminating TSA's need to rescreen baggage that was previously screened at the Last Point of Departure (LPD) for cleared passengers. As TSA looks to support a One Stop Security approach, the ability to implement remote screening will be instrumental.

Leveraging this capability has the potential to improve overall effectiveness and operational efficiency for checked baggage screening by improving throughput and reducing TSOs' cognitive burden. Also, remote screening could allow airports to handle increased passenger and checked baggage volume as a result of future growth and support continuity of operations during national emergencies. Additionally, efforts to enable secure data transmission would allow TSA to explore and use international standards and data-sharing agreements with foreign governments to enhance detection and decrease duplicative baggage screening with trusted partners.

As Checked Baggage continues to build the next generation of capability requirements, there is intent to leverage and incorporate TSE R&D investments from existing initiatives in system architecture, data transfer, and connectivity requirements.

Enable

The third identified function of the Checked Baggage Capability refers to efforts that facilitate future enhancements of existing and emerging technology. The capability future state is to leverage an Open Architecture concept and move towards enhanced capabilities such as Selectee Screening Automation, Common Workstation, remote data transmission, leveraging third party algorithms and Threat Image Projection (TIP).

Dynamic Screening: Selectee Screening Automation

TSA is interested in conducting a demonstration and proof of concept in order to achieve Dynamic Screening. Selectee Screening Automation is the first iteration RCA is focusing on, that is, routing selectee passengers' baggage to the Checked Baggage Resolution Area (CBRA). This state-of-the-art screening system will integrate technologies, capabilities, and procedures across the Checked Baggage environment. The results of this study will determine security effectiveness improvements and efficiency gains for future Dynamic Screening implementation.

Common Workstation and DICOS

TSA aims to develop a common workstation for Checked Baggage to increase TSO deployment flexibility and optimize training. The common workstation will be comprised of three parts: a common graphical user interface (CGUI) to standardize the look and feel of the machine interface, a standard imaging format to be used by all OEMs, and standardized data exchange interfaces. The first iteration is currently under development. TSA also looks to standardize imaging format using the Digital Imaging and Communication in Security (DICOS) format across the TSA enterprise, allowing for improved data sharing thus enabling the future vision of specialized screening operations (remote screening). Standardized data exchange interfaces will allow TSA to plug-and-play with different types of common workstations and more easily upgrade systems across the fleet to improve operator performance.

Furthermore, TSA seeks to implement a common training platform that will comprise all CGUI formats and functions that TSOs use every day.

As Checked Baggage continues to build the next generation of capability requirements, there is intent to leverage and incorporate TSE R&D investments from existing initiatives in system architecture, data transfer, and connectivity requirements to implement Common Workstation and DICOS.

Threat Image Projection

TSA is also planning on deploying Threat Image Projection (TIP) in the Checked Baggage environment, which will involve randomly presenting fictional threat images to TSOs in the operational setting with a predefined frequency. The EDS portion of TIP will be a developmental software to support the monitoring of screener performance, the measurement of operator performance, and the assessment of operator training effectiveness. TIP results will provide a feedback loop to consistently evaluate Tactics, Techniques, and Procedures (TTP) and inform security effectiveness.

As TSA continues to deploy CT systems for Checkpoint operations, Checked Baggage will be able to leverage R&D investments and capability deployments from Accessible Property Screening to implement TIP.

Checked Baggage Strategic R&D Investments

Figure 1 illustrates the gradual maturation of the three functions of Checked Baggage through the four phases:

**Figure 1: Mapping Checked Baggage Technologies Maturation*

	FY22 - FY23	FY24 - FY25	FY26 - FY27	FY28+
Detect	• Release Detection Standard 8.0 to OEMs • Analyze threat preference/ characterization needed to realize 8.0 Detection Standard	• Initiate R&D for XRDs and DPCs • Funding capability development and testing of advanced threat detection algorithms to increase security effectiveness, with a focus on leveraging Open Architecture enablers to support a diverse marketplace	• Develop requirements for XRDs for EDS Platforms • Funding capability development and testing of advanced threat detection algorithms to increase security effectiveness	• Demonstrate XRDs • Funding capability development and testing of advanced threat detection algorithms to increase security effectiveness
Connect	• Develop Remote Screening requirements (International to Domestic)	• Test and demonstrate Remote Screening capabilities • Define data architecture and requirement needs for CB mission space	• Implement Remote Screening capabilities	• Scale Remote Screening capabilities
Enable	• Release DICOS 3.0 Standard to enable Open Architecture • Initiate R&D for TIP	• Update Requirements to include DICOS 3.0 • Explore the use of standardized interfaces and communication protocols • Develop requirements and demonstrate TIP	• Develop Open Architecture artifacts and processes to include Common Image Format, Common Tools, and Remote Screening • Test, procure, deploy, and maintain TIP	• Implement and scale Open Architecture artifacts and processes to include Common Image Format, Common Tools, and Remote Screening • Maintain TIP

*Currently, RCA Checked Baggage has no programmed funds. These efforts are pending availability of funds.

Stakeholder Collaboration

TSA seeks to collaborate with internal and external stakeholders throughout the Checked Baggage Capability maturation process as well as development of this Roadmap.

Internal Stakeholder Coordination

Within TSA, the Checked Baggage CM and Program manager (PM) engage with the following stakeholders in the development and maturation of Checked Baggage capabilities.

- **Requirements Development Branch** – Capturing non-materiel and materiel courses of action to address Checked Baggage needs and developing user-level requirements for materiel solution acquisitions
- **Capability Development Integration Branch** – Coordinate and conduct systems engineering activities to develop and mature Checked Baggage technologies to advance TSA's security and screening capabilities.
- **Human Performance Branch** – Improve human performance and experience for operators of Checked Baggage (for example, security effectiveness, efficiency, morale).
- **Innovation Task Force** – Foster innovation by integrating key stakeholders to identify and demonstrate emerging solutions that increase security effectiveness and efficiency.
- **Training & Development** – Provide training and best practices to TSOs to improve security posture in the Checked Baggage environment.
- **Information Technology** – Manage the development and implementation efforts for network connectivity capability development and define and vet cybersecurity requirements through the Chief Information Security Officer (CISO).
- **Security Operations** – Responsible for the security of the nation's transportation systems to ensure freedom of movement for people and commerce, including Checked Baggage screening operations.
- **Testing and Evaluation Division** – Provide both Test and Evaluation and support services throughout the technology procurement lifecycle for technology in the Checked Baggage environment.
- **Deployment Logistics Division** – Develop and execute deployment strategies for screening technologies in the Checked Baggage environment.
- **Chief Finance Office** – Provide financial and administrative support to the Checked Baggage Capability.

External Stakeholder Coordination

DHS Coordination

The Checked Baggage Capability also sits within the greater DHS mission context. TSA is collaborating with the DHS Science & Technology (S&T) Directorate to identify R&D opportunities that support and align to Checked Baggage's Capability goals. This collaboration seeks to develop consensus around a set of technology needs and capabilities required to satisfy those needs for Checked Baggage. It allows TSA and S&T to align development and acquisition strategies to technology readiness and identify early pilot, demonstration, and transition/deployment opportunities. S&T strives to develop state-of-the-art automated high-speed, high-performance Checked Baggage EDS with improved material discrimination/identification, increased throughput, and reduced operations and maintenance costs for TSA acquisition.

TSA, S&T, and the Homeland Security Operational Analysis Center (HSOAC) conducted a study to determine the future of the Checked Baggage mission space. That study informed this Capability Roadmap, the future of EBSP, and industry focus.

Industry

In order to advance Checked Baggage capabilities, TSA plans to continue use of multiple methods to engage with industry. An example of this industry engagement is the Innovative Demonstrations for Enterprise Advancement (IDEA) Targeted Broad Agency Announcement (BAA) which is completed by TSA's Innovation Task Force (ITF). The ITF IDEA BAA aims to identify and promote the demonstration of diverse, forward-looking solutions or processes that increase TSA's security capabilities. ITF works with industry partners and academic institutions to demonstrate capabilities in live airport environments, consistent with TSA's strategic priority to accelerate time to field new capabilities. Overall, the Checked Baggage capability intends to utilize TSA's existing ITF processes and BAA's to support the development and demonstration of future requirements for the next generation of EDS. While funds are not currently available to support this effort, a partnership with DHS S&T will be leveraged to complete the targeted investment.

International

TSA continues to collaborate with its international counterparts to identify and leverage best practices for Checked Baggage development and deployment. RCA is exploring opportunities for data-sharing with trusted foreign governments to raise the global baseline.

TSA's Trade Space Framework

When making decisions about future Checked Baggage capabilities, the potential impact to the mission's five key components of the TSA Trade Space Framework are evaluated:

- Security Effectiveness
- Operational Efficiency
- Passenger Satisfaction
- Industry Vitality
- Fiscal/Policy Issues

Figure 2: TSA's Trade Space Framework

By considering the impacts across the Trade Space, the agency can drive investment decisions based on a holistic review of identified key factors. To accomplish TSA's future vision, TSA, industry, and academic partners could invest in several capabilities to achieve the goals of the Trade Space framework.

Security Effectiveness: Security Effectiveness is a measure of integrated, real-world performance in security screening according to a defined set of criteria designed to selectively identify and mitigate threats within a protected area. The Checked Baggage Capabilities means of improving security effectiveness includes improving existing EDS machines, advancing threat detection algorithms, and reducing false alarm rates.

Operational Efficiency: Operational Efficiency is the capacity of systems (technology and process) to maintain Security Effectiveness by streamlining core processes and developing and implementing screening solutions in the most cost-effective manner possible. As TSA screens and processes an average of 1.4 million checked bags every day across the United States, investment in Checked Baggage is targeted to expedite baggage processing times and throughput.

Passenger Satisfaction: Passengers are indirectly involved with Checked Baggage screening technologies. However, as TSA improves operational efficiency and system capabilities, limiting the amount of checked baggage requiring physical search, passenger satisfaction will also improve.

Industry Vitality: TSA strives to support industry vitality by working in partnership with airports, airlines, service contractors, and equipment manufacturers that make investment choices based on collective security benefits as well as their own economic interests and incentives. Together, this group will determine the impacts of investments such as the paradigm shift between the current state and future state of Checked Baggage capabilities.

Fiscal/Policy Issues: TSA assesses the feasibility of future Checked Baggage screening capabilities under the current policy and fiscal landscape. RCA will continue devising innovative and cost-effective measures to improve Checked Baggage screening with the goal of reducing procurement, deployment, and maintenance costs.


RC2-05
RC1-05
KLM

Conclusion

The threats to transportation security and checked baggage aviation security are continuously evolving and more complex than ever before. These challenges include the proliferation of new technologies, development of new weapons and tactics that are more difficult to counter, and persistence and adaptability of adversaries. TSA must be flexible, adaptable, and responsive to quickly address these emerging threats. TSA will use every tool at its disposal to address these challenges and associated risks by developing methods to combat them such as enhanced procedures and capabilities to deter, detect, and prevent attacks. Open Architecture will provide the needed flexibility and increase the likelihood of delivering needed capabilities to the field.

This Roadmap serves to define and highlight the possible evolution and development areas of Checked Baggage screening capabilities. With the collaboration of the innovative and technological arms of TSA, its government partners, industry, and academia, Checked Baggage security will see marked evolutionary improvements to travel safety and security while facilitating the flow of people and commerce.

Glossary

Term	Definition
Checked Baggage	Checked Baggage includes property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during the flight. Accompanied commercial courier consignments are not classified as Checked Baggage.
Checkpoint Baggage Screening System	A type of transportation security equipment that integrates both threat detection and article handling capabilities for screening articles at airport checkpoints.
Differential Phase Contrast (DPC)	DPC provides a tri-signature derived from three independent material property measurements: standard absorption; index of refraction; and dark field scattering; to produce an image that can then be processed and analyzed for automated material identification.
Digital Imaging and Communication in Security (DICOS)	DICOS is an extensible, interoperable, data standard that enables the integration of disparate security screening imaging technologies, images, and related data.
Explosives Detection System (EDS)	Explosives Detection Systems are automated systems that scan checked baggage and analyze the contents to determine whether explosive threats might be present. The automated systems streamline the checked baggage screening process at airports nationwide.
Explosives Trace Detection (ETD)	When a baggage screener swabs a bag and then inserts the swab into the ETD machine, this can detect chemical residues that may indicate the presence of explosives within a bag.
Electronic Baggage Screening Program (EBSP)	The Electronic Baggage Screening Program was established by congressional mandate for screening of all passenger checked baggage for concealed explosives. The program achieves this mission by managing the full life cycle of acquisition activities including requirements identification, testing, procurement, deployment and sustainment of screening equipment.
False Alarm	Where the machine registers an alarm for a bag that is found to be benign.
Open Architecture (OA)	OA is a design approach where components, such as software and hardware, are standards-based and interoperable to allow any vendor to create improved subcomponents (e.g. new detection algorithms, user interfaces, reporting systems, etc.) to create a superior combined system.

Term	Definition
Threat Image Projection (TIP)	TIP is a software solution that projects fictional images of actual threats on screening equipment alongside live stream of commerce baggage.
Throughput	Throughput is defined as the number of checked bags screened per hour.
X-ray Diffraction (XRD) Technology	X-ray imaging provides a major tool in checked baggage inspection, with various sensitive techniques being brought to bear in determining the form, and density of items within luggage as well as other material dependent parameters.

@TSA @TSA facebook.com/TSA