Capital Investment Plan

FY 2025–FY 2029

October 3, 2024

Fiscal Year 2024 Report to Congress

Homeland Security

Transportation Security Administration

Message from the Administrator

October 3, 2024

I am pleased to present the following "Capital Investment Plan" (CIP) for fiscal year (FY) 2025 – FY 2029, which was prepared by the Transportation Security Administration (TSA).

TSA compiled the CIP according to reporting requirements in the FY 2024 Department of Homeland Security (DHS) Appropriations Act (P.L. No. 118-47), and the accompanying Joint Explanatory Statement; Senate Report 115-283 accompanying the FY 2019 DHS Appropriations Act (P.L. 116-6); and the Transportation Security Acquisition Reform Act (P.L. 113-245). This single, annual report presents TSA's plan for continuous and sustained investments in new, and the replacement of aged transportation security equipment (TSE), and other capital investments. In addition, as required by these reporting requirements, TSA also included an unconstrained CIP, as mandated by Congress, which reflects the Agency's ability to invest in executable technology solutions if budget constraints were not a factor. This constitutes a significant change from the FY 2024-2028 CIP, which also included the required unconstrained portion.

As TSA's risk landscape evolves, TSA must continue to invest in, acquire, and field new technologies to strengthen transportation security, partnering with other DHS Components and industry partners in aviation and surface transportation to drive innovation and modernization. The CIP provides a cohesive view of transportation security investments necessary to achieve TSA's strategic priorities within the context of its operational environment and threat landscape. The CIP serves as TSA's guide when determining and prioritizing future investments to fulfill critical missions.

Pursuant to Congressional reporting requirements, this report is being provided to the following Members of Congress:

The Honorable Tom Cole
Chairman, House Committee on Appropriations

The Honorable Rosa L. DeLauro
Ranking Member, House Committee on Appropriations

The Honorable Patty Murray
Chair, Senate Committee on Appropriations

The Honorable Susan M. Collins
Vice Chair, Senate Committee on Appropriations

The Honorable Mark E. Green
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Maria Cantwell
Chair, Senate Committee on Commerce, Science, and Transportation

The Honorable Ted E. Cruz
Ranking Member, Senate Committee on Commerce, Science, and Transportation

Inquiries relating to this report may be directed to me at (571) 227-2801 or TSA's Legislative Affairs office at (571) 227-2717.

Sincerely,

David P. Pekoske
Administrator

Executive Summary

The transportation sector remains a significant target for malicious actors, due to the prevalence of soft targets within the sector, public accessibility of many transportation modes, and the importance of transportation infrastructure to the Nation. International and domestic terrorists and state and non-state actors pose a variety of physical and cyber threats[1] against all aspects of critical infrastructure. TSA continues to monitor this evolving threat environment, while managing associated risks. Risk-based decision-making is inherent to TSA's mission of protecting the Nation's transportation systems, to ensure the freedom of movement for people and commerce. Challenges and risks TSA encounters remain complex; therefore, TSA must maintain a long-term, strategic view in response to risks and solutions.

While personnel are critical to the success of capital investments, the FY 2025 – FY 2029 CIP outlines TSA's strategy for executing its mission with continuous and sustained investment within base funding. The CIP provides Congressional stakeholders with not only a guide to current strategic investments, but also discusses the extent to which TSA could maximize those capabilities. In the current budgetary constrained environment, the CIP Appendix A demonstrates how TSA continues to advance strategic priorities by investing in, acquiring, and fielding new technologies and enhancing information technology (IT) systems, through new and existing contracts that strengthen security effectiveness and efficiency. The 'Unconstrained' investment opportunities section highlights TSA's current investments in checkpoint and checked baggage TSE, how TSA could enhance these capabilities with additional investments, and highlights their importance to TSA's mission.

TSA by the Numbers

According to the International Air Transport Association, the global aviation industry is expected to experience a significant increase in the number of travelers in 2024, surpassing pre-pandemic (2019) levels.[2] To meet this demand, TSA maintains responsibility for the security of 440 federalized airports servicing over 23,000 domestic flights and nearly 2,600 outbound international flights per day. Additionally, TSA screens more than 858 million passengers annually and over 1.9 billion carry-on and checked items for explosives and other dangerous items. TSA ensures aviation travel adheres to regulatory compliance via the work conducted by more than 600 aviation transportation security inspectors.

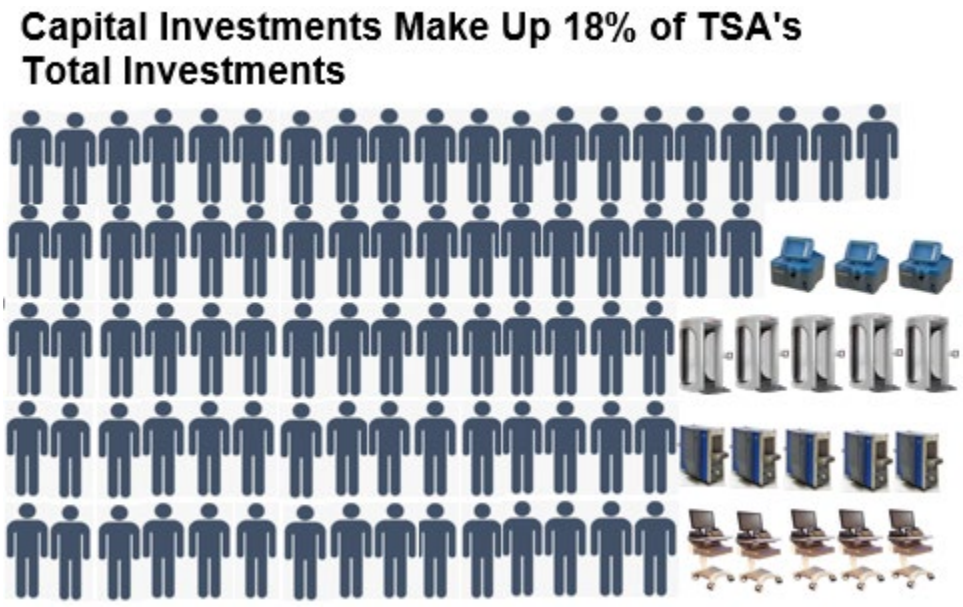
Within the surface network, TSA conducts work that connects cities, manufacturers, and retailers through more than 4 million miles of roadways; nearly 140,000 miles of railroad track; approximately 612,000 bridges and more than 470 tunnels; approximately 360 maritime ports, over 3,700 marine terminals, approximately 12,000 miles of coastline; and approximately 2.7 million miles of pipeline. Eight thousand surface regulatory inspections are conducted annually in support of risk-based security and nearly 30 million daily trips taken on public transportation.

[1] FBI director warns that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure
[2] IATA - Global Air Travel Demand Continued Its Bounce Back in 2023

Continuous and Sustained Investment

TSA continues to invest in, acquire, and field new, sustainable solutions, despite most funds dedicated towards non-capital investments (see **Figure 1**).

Figure 1: TSA's Capital Investments Exceeded by Non-Capital Expenditures



Innovative security technologies, collaboration between stakeholders, a well-trained and dedicated security workforce, and a proactive approach to preparedness and resilience all help shape these investments. The CIP covers the next 5 fiscal years' planned obligations and is based on the Future Years Homeland Security Program (FYHSP) authorized levels.[3] The CIP provides a cohesive overview of capital investments required: to achieve TSA's strategic priorities; to adapt to disruptions in the transportation ecosystem; and to address complex future challenges within the FYHSP. In addition, the CIP provides an 'unconstrained' view of TSE and mission capabilities if TSA was not operating in a constrained budget environment. **Figure 2** outlines TSA's FY 2025 budget request.

[3] Throughout a given fiscal year, requirements may be reprioritized based on changes in the threat environment, operational needs, programmatic reviews, leadership priorities, or other circumstances. Resource levels in the FYHSP may change to align with TSA's changing priorities through the annual budget process.

Figure 2: TSA Budget Request FY 2025

TSA Budget Request FY 2025 (Dollars in Thousands)								
	2023 Enacted		2024 Enacted		2025 President's Budget		2024 - 2025 Total Changes	
	FTE	$0	FTE	$0	FTE	$0	FTE	$0
Operations and Support	55,788	$6,308,363	58,232	$6,744,968	58,271	$6,475,065	39	($269,903)
Procurement, Construction, and Improvements		$141,645	0	$40,678		$98,912	0	$58,234
Research and Development		$33,532	0	$14,641		$17,990	0	$3,349
Net Discretionary	**55,788**	**$6,483,540**	**58,232**	**$6,800,287**	**58,271**	**$6,591,967**	**39**	**-208,320**
Aviation Passenger Security Fee		$2,490,000		$3,420,000		$4,404,400	0	$984,400
Vetting Fees - Discretionary	386	$311,750	386	$350,000	401	$552,650	15	$202,650
Gross Discretionary	**56,174**	**$9,285,290**	**58,618**	**$10,570,287**	**58,672**	**$11,549,017**	**54**	**$978,730**
Flight Training Security Program	19	$6,000	19	$6,000	19	$6,000	0	$0
Aviation Security Capital Fund		$250,000		$250,000		$250,000	0	$0
Total Mandatory/Fees	**19**	**$256,000**	**19**	**$256,000**	**19**	**$256,000**	**0**	**$0**
Total Budget Authority	**56,193**	**$9,541,290**	**58,637**	**$10,826,287**	**58,691**	**$11,805,017**	**54**	**$978,730**
Less: Rescissions to Prior Year Balances		-$12					0	$0
Appropriated Funds	**56,193**	**$9,541,278**	**58,637**	**$10,826,287**	**58,691**	**$11,805,017**	**54**	**$978,730**

Note: FTE denotes Full-Time Employees

Sustainment and Acquisition Lifecycle

TSA operates both new and legacy TSE while evaluating potential affordable replacements for the latter. TSE sustainment remains a large proportion of TSA's capital investments and demands continued resourcing to counter annual cost increases such as continuous deployments and inflation. Therefore, it remains a strategic priority and focus area. **Figure 3** reflects the resources required to ensure the full TSE suite is maintained and operational at all US airports.

Figure 3: TSA Maintenance Funding Profile

TSA Security Equipment Sustainment – FY 2025 - FY 2029 ($ in millions)						
	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 - 2029 Total
Advanced Imaging Technology (AIT)	$32.9	$33.5	$34.0	$34.5	$35.1	$170.0
Advanced Technology (AT)	$62.0	$63.0	$64.0	$65.0	$66.1	$320.1
Checkpoint Property Screening System (CPSS)	$10.4	$10.7	$10.9	$11.2	$11.4	$54.6
Credential Authentication Technology (CAT)	$6.4	$6.6	$6.7	$6.9	$7.1	$33.7
Electronic Baggage Screening Program (EBSP)	$256.2	$260.3	$264.5	$268.7	$273.0	$1,322.7
Explosive Trace Detector (ETD)	$44.4	$45.1	$45.8	$46.6	$47.3	$229.2
Passenger Screening Program Legacy (PSP)	$12.3	$12.5	$12.7	$12.9	$13.1	$63.5
Non Investment	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0
Total TSA Security Equipment Maintenance	**$424.6**	**$431.7**	**$438.6**	**$445.8**	**$453.1**	**$2,193.8**
FY 2025 reflects President's Budget, and FY 2026-2029 are estimated amounts						

To supplement TSA's Acquisition Manual (TSAAM) issued in 2018, TSA is developing an Open Architecture (OA) Acquisition Guidebook highlighting OA and System of Systems (SoS) concepts applicable within the phases and activities of the Acquisition Lifecycle Framework

(ALF).[4] The TSAAM outlines a repeatable, transparent, and flexible acquisition process, and TSA leverages it to implement concepts such as OA and SoS.

As a keystone manual for TSA acquisitions, TSAAM provides the foundational information that acquisition teams need to deliver the right capability in a timely manner through the following acquisition lifecycle phases.

- **Aligning Resources in Pre-Need -** The Pre-Need Phase is a prerequisite for entering the ALF. In this phase, TSA collects, analyzes, and prioritizes TSA capability gaps.

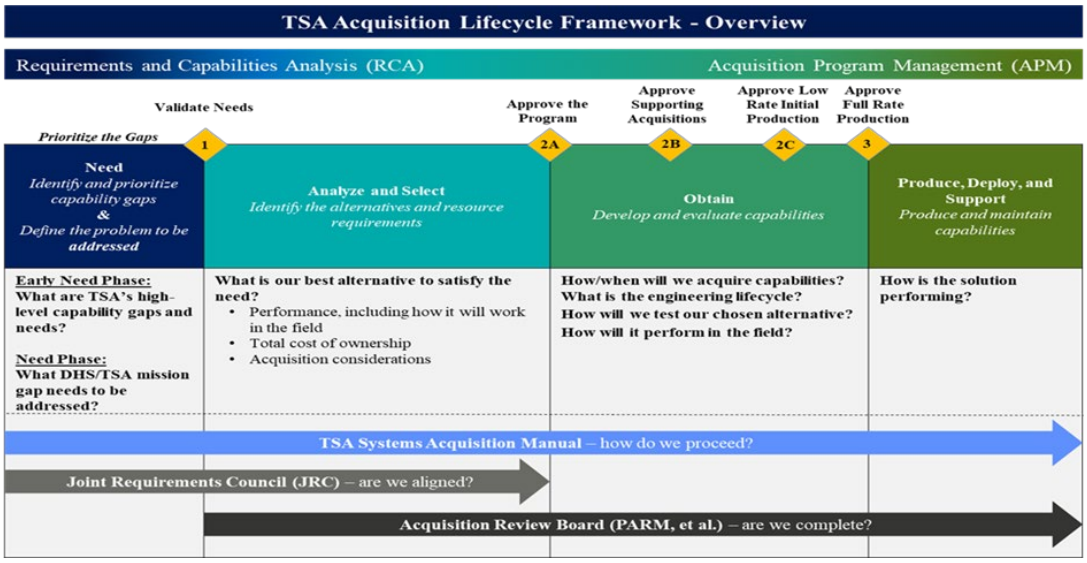
- **Identifying Needs -** In this phase, TSA validates the need for the prospective acquisition, ensures alignment of the prospective acquisition to TSA and DHS objectives, defines the mission need, and develops initial requirements.

- **Analyzing and Selecting Alternatives -** During this phase, TSA facilitates testing and evaluation of potential capabilities, analyzes alternatives, and estimates the costs of prospective acquisitions, culminating in the decision to officially approve or disapprove a prospective acquisition.

- **Leveraging Department Efficiencies -** DHS strategic sourcing contracting vehicles provide DHS Components with economic and performance benefits through collaboration and enterprise planning. TSA continues to embrace strategic sourcing as a proven best practice to save money, reduce redundancy, drive standardization, streamline procurements, and improve business efficiency.

- **Obtain -** TSA focuses on systems development, testing, and evaluation to ensure an effective acquisition through improving agile processes, accelerating capability delivery, and reducing costs.

[4] DHS Acquisition Management Instruction 102-01-001, rev. 01 (March 9, 2016) and DHS Manual for the Operation of the Joint Requirements Integration and Management System, rev. 00 (April 21, 2016).



Strategic Alignment

The CIP is TSA's long-term roadmap that aims to align capital expenditures with larger strategic goals. The plan supports and informs the TSA Strategy, the Administrator's Intent, roadmaps (for example, Identity Management, Cybersecurity, Insider Threat, Air Cargo Security, OA), and Strategic Priorities and Planning Guidance.

To achieve TSA's strategic vision, TSA aligns its capital investments with the following focus areas, displayed in **Figure 4**:

1) Identity Management and Vetting
2) Threat Detection System-of-Systems
3) Enhanced and Secure IT Systems

Figure 4: CIP Summary Table FY 2025 – FY 2029

CIP FY 2025 - FY 2029 ($ in millions)								
Program	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 - 2029 Total	FOC (Past and Future)	Total Currently Deployed
A. Vetting and Biometrics								
Technology Infrastructure Modernization (TIM)	$80.4	$80.7	$81.0	$81.3	$81.5	**$404.9**	**15-Jul-19**	**N/A**
Secure Flight	$146.4	$153.7	$157.6	$160.7	$163.8	**$782.2**	**15-Jul-09**	**N/A**
Credential Authentication Technology (CAT)	$18.9	$19.0	$19.3	$19.5	$19.7	**$96.4**	**31-Mar-49**	**2,054**
Identity Management	$3.2	$7.3	$7.4	$7.4	$7.4	**$32.7**		**N/A**
A. Vetting and Biometrics SubTotal	**$248.9**	**$260.7**	**$265.3**	**$268.9**	**$272.4**	**$1,316.2**		
B. Threat Detection System-of-Systems								
Accessible Property Screening (APS)	$0.6	$0.6	$0.6	$0.6	$0.6	**$3.0**		**N/A**
Checkpoint Property Screening System (CPSS)	$144.7	$145.4	$146.3	$147.2	$148.1	**$731.7**	**30-Sep-36**	**N/A**
Advanced Technology (AT) - Computed Tomography Systems	$72.7	$73.9	$75.1	$76.3	$77.5	**$375.5**	**30-Dec-16**	**777**
Explosives Trace Detection (ETD)	$49.5	$50.3	$51.1	$51.9	$52.8	**$255.6**		**5,874**
Alarm Resolution	$6.1	$6.8	$7.1	$7.2	$7.2	**$34.4**		**N/A**
Advanced Imaging Technology (AIT)	$37.9	$38.5	$39.1	$39.7	$40.4	**$195.6**	**1-Sep-17**	**1,059**
On-Person Detection/Next Gen Advanced Imaging Technology (AIT)	$9.3	$9.4	$9.5	$9.6	$9.7	**$47.5**		**N/A**
Electronic Baggage Screening Program (EBSP)	$282.9	$287.5	$292.1	$296.7	$301.5	**$1,460.7**	**31-Dec-03**	**1,626**
Checked Baggage	$1.1	$1.0	$1.0	$1.0	$1.0	**$5.1**		**N/A**
ASCF - Electronic Baggage Screening Program (EBSP)	$250.0	$250.0	$250.0	$250.0	$250.0	**$1,250.0**		**N/A**
Multimodal and Public Area Capabilities	$21.4	$21.6	$21.9	$22.1	$22.4	**$109.4**		**N/A**
Counter-Unmanned Aerial Systems	$11.6	$11.8	$12.0	$12.1	$12.2	**$59.7**		**N/A**
National Explosives Detection Canine Team Program	$162.6	$167.3	$171.7	$176.1	$180.6	**$858.3**		**1,103**
B. Threat Detection System-of-Systems Subtotal	**$1,050.4**	**$1,064.1**	**$1,077.5**	**$1,090.5**	**$1,104.0**	**$5,386.5**		
C. Enhanced and Secure IT Systems								
IT Infrastructure Program	$390.2	$396.8	$403.7	$410.7	$417.7	**$2,019.1**	**30-Sep-08**	**N/A**
Cyber Security	$157.4	$174.4	$175.5	$176.8	$178.1	**$862.2**		**N/A**
Field Information Systems (FIS)	$36.1	$36.7	$37.2	$37.8	$38.4	**$186.2**	**1-Jul-19**	**N/A**
Enterprise Physical Access Control System	$10.5	$10.6	$10.8	$11.0	$11.2	**$54.1**		**N/A**
Human Capital IT Modernization	$146.8	$152.0	$154.5	$156.9	$159.3	**$769.5**	**30-Jun-19**	**N/A**
Staffing, Scheduling, Time, and Attendance System	$18.3	$18.4	$18.5	$18.7	$18.8	**$92.7**		**N/A**
Air Cargo IT Systems	$13.3	$13.5	$13.8	$14.0	$14.2	**$68.8**	**31-Dec-10**	**N/A**
C. Enhanced and Secure IT Systems Subtotal	**$772.6**	**$802.4**	**$814.0**	**$825.9**	**$837.7**	**$4,052.6**		
Total	**$2,071.9**	**$2,127.2**	**$2,156.8**	**$2,185.3**	**$2,214.1**	**$10,755.3**		

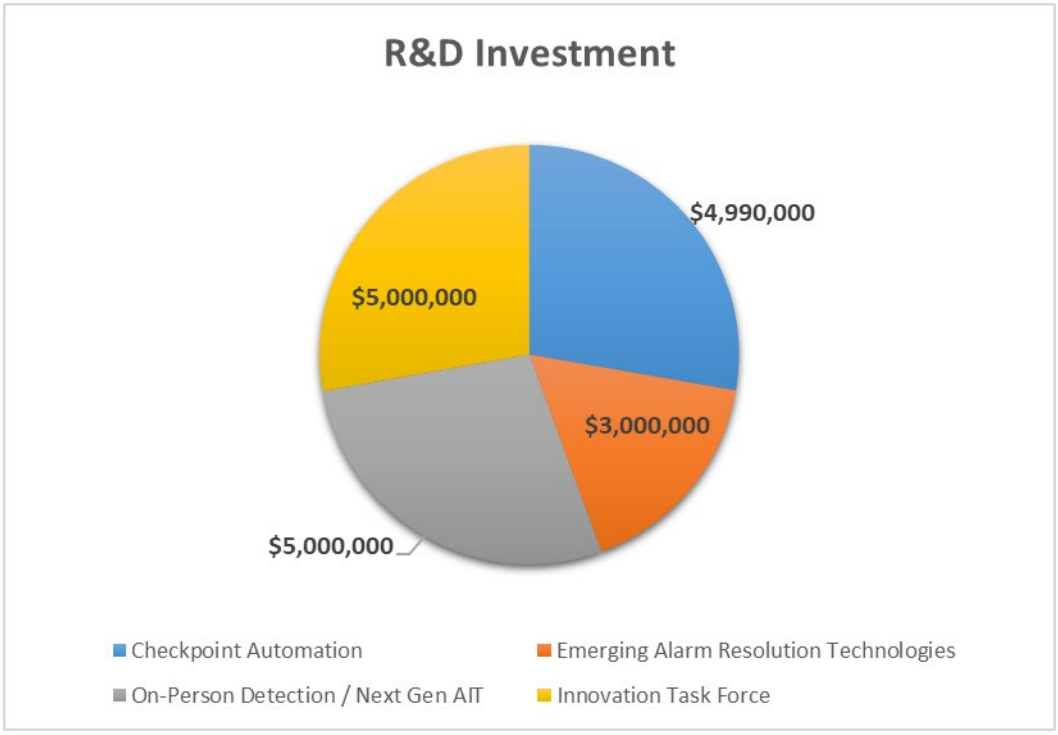
Note: Figure 4 reflects the FY 2025 Congressional Justfication Funding Guidance.

Need for Long-Term Investment

Looking to the future, TSA requires productive and diverse partnerships with stakeholders from industry, government, and academia. These partnerships are essential to improve security effectiveness, ecosystem-wide innovation, operational efficiency, customer experience, and workforce capabilities.

TSA's mission success depends on simultaneous investment in capital assets and in R&D. This includes applied research, development, testing, and evaluation activities that advance innovative technology solutions and support TSA's security infrastructure. Although funding is limited, TSA continues to benefit from partnerships with other Federal Government departments and agencies such as the DHS Science and Technology Directorate and the Department of Defense. The planned distribution of the FY 2025 R&D funds, totaling $18 million, is shown in **Figure 5**.

Figure 5: R&D Investment FY 2025



Capital Investment Plan
FY 2025–FY 2029

Table of Contents

I. Legislative Language

This report addresses reporting requirements in the Joint Explanatory Statement accompanying the Fiscal Year (FY) 2024 Department of Homeland Security (DHS) Appropriations Act (P.L. 118-47) and its accompanying Joint Explanatory Statement; Senate Report 115-283 accompanying the FY 2019 DHS Appropriations Act (P.L. 116-6); and the Transportation Security Acquisition Reform Act (P.L. 113-245).

The FY 2024 DHS Appropriations Act (P.L. 118-47) includes the following requirements:

> Section. 220. Not later than 45 days after the submission of the President's budget proposal, the Administrator of the Transportation Security Administration shall submit to the Committees on Appropriations and Homeland Security of the House of Representatives and the Committees on Appropriations and Commerce, Science, and Transportation of the Senate a single report that fulfills the following requirements:
> (1) a Capital Investment Plan, both constrained and unconstrained, that includes a plan for continuous and sustained capital investment in new, and the replacement of aged, transportation security equipment;
> (2) the 5-year technology investment plan as required by section 1611 of title XVI of the Homeland Security Act of 2002, as amended by section 3 of the Transportation Security Acquisition Reform Act (Public Law 113–245); and
> (3) the Advanced Integrated Passenger Screening Technologies report as required by the Senate Report accompanying the Department of Homeland Security Appropriations Act, 2019 (Senate Report 115–283).

The Joint Explanatory Statement includes the following provision:

> Section 220. The agreement continues a provision requiring TSA to provide a report that includes the Capital Investment Plan, the five-year technology investment plan, and information on Advanced Integrated Passenger Screening Technologies.

Senate Report 115-283 provides:

> *Advanced Integrated Screening Technologies*.—TSA is directed to submit a detailed report on passenger and baggage screening technologies not later than 180 days after the date of enactment of this act. The report shall include a useful description of existing and emerging technologies capable of detecting threats concealed on passengers and in baggage, as well as projected funding levels for each technology identified in the report for the next five fiscal years.

The Transportation Security Acquisition Reform Act (P.L. 113-245) provides further guidance:

SEC. 1611. 5-YEAR TECHNOLOGY INVESTMENT PLAN.

(a) IN GENERAL. —The Administrator shall—

(1) not later than 180 days after the date of the enactment of the Transportation Security Acquisition Reform Act, develop and submit to Congress a strategic 5-year technology investment plan, that may include a classified addendum to report sensitive transportation security risks, technology vulnerabilities, or other sensitive security information; and

(2) to the extent possible, publish the Plan in an unclassified format in the public domain.

(b) CONSULTATION. —The Administrator shall develop the Plan in consultation with—

(1) the Under Secretary for Management;

(2) the Under Secretary for Science and Technology;

(3) the Chief Information Officer; and

(4) the aviation industry stakeholder advisory committee established by the Administrator.

(c) APPROVAL. —The Administrator may not publish the Plan under subsection (a)(2) until it has been approved by the Secretary.

(d) CONTENTS OF PLAN. —The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by security-related technology, including consideration of the most recent quadrennial homeland security review under section 707;

(2) a set of security-related technology acquisition needs that—

(A) is prioritized based on risk and associated capability gaps identified under paragraph (1); and

(B) includes planned technology programs and projects with defined objectives, goals, timelines, and measures;

(3) an analysis of current and forecast trends in domestic and international passenger travel;

(4) an identification of currently deployed security-related technologies that are at or near the end of their lifecycles;

(5) an identification of test, evaluation, modeling, and simulation capabilities, including target methodologies, rationales, and timelines necessary to support the acquisition of the security-related technologies expected to meet the needs under paragraph (2);

(6) an identification of opportunities for public-private partnerships, small and disadvantaged company participation, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer;

(7) an identification of the Administration's acquisition workforce needs for the management of planned security-related technology

acquisitions, including consideration of leveraging acquisition expertise of other Federal agencies;

(8) an identification of the security resources, including information security resources, that will be required to protect security-related technology from physical or cyber-enabled theft, diversion, sabotage, or attack;

(9) an identification of initiatives to streamline the Administration's acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation;

(10) an assessment of the impact to commercial aviation passengers;

(11) a strategy for consulting airport management, air carrier representatives, and Federal security directors whenever an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with such officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations; and

(12) in consultation with the National Institutes of Standards and Technology, an identification of security-related technology interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems.

(e) LEVERAGING THE PRIVATE SECTOR. —To the extent possible, and in a manner that is consistent with fair and equitable practices, the Plan shall—

(1) leverage emerging technology trends and research and development investment trends within the public and private sectors;

(2) incorporate private sector input, including from the aviation industry stakeholder advisory committee established by the Administrator, through requests for information, industry days, and other innovative means consistent with the Federal Acquisition Regulation; and

(3) in consultation with the Under Secretary for Science and Technology, identify technologies in existence or in development that, with or without adaptation, are expected to be suitable to meeting mission needs.

(f) DISCLOSURE. —The Administrator shall include with the Plan a list of nongovernment persons that contributed to the writing of the Plan.

(g) UPDATE AND REPORT. —Beginning 2 years after the date the Plan is submitted to Congress under subsection (a), and biennially thereafter, the Administrator shall submit to Congress—

(1) an update of the Plan; and

(2) a report on the extent to which each security-related technology acquired by the Administration since the last issuance or update of the Plan is consistent with the planned technology programs and projects identified under subsection (d)(2) for that security-related technology.

II. Plan Overview

The Capital Investment Plan (CIP) provides a cohesive view of transportation security investments necessary to achieve TSA's strategic priorities in operational and threat environments. The CIP will transform TSA's execution of transportation security coupled with risk-based policy changes, process improvements, and strategic partnerships.

The FY 2025 – FY 2029 CIP summarizes TSA's efforts to plan strategically and to improve transportation security continuously, specifically security solutions like transportation security equipment (TSE), information technology (IT) infrastructure, and other capital investments.

Furthermore, following the President's Executive Order (EO) 14058, "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government,"[5] continuous improvements in transportation security solutions aim to improve service delivery and customer experience as fundamental priorities. These improvements also help to ensure that protections afforded under the law are maintained appropriately.

In FY 2025, the Federal Government will operate under strict caps agreed to in the Fiscal Responsibility Act of 2023. This requires a more austere approach that addresses must-pay expenditures, maintaining current services, and constricting budgetary growth to the greatest possible extent. The plan describes a future state in which TSA reduces risk to the transportation sector by maximizing investments.

[5] EO on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on- transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

III. Strategic Priorities to Drive Mission Execution

Throughout the FY 2025 – FY 2029 requirements prioritization process, TSA considered the TSA Strategy and the Administrator's Intent 3.0 with three key strategic priorities: people, partnership, and technologies. The CIP outlines capital investments that drive these priorities through the funding provided by Congress, defines the TSA mission space and how to address capability needs and gaps, and identifies current limitations and how to improve with more investment and fully funding our capabilities.

A. Identifying and Prioritizing Threats, Risks, and Capability Needs and Gaps

TSA continues advancing transportation security capabilities in high- risk areas. TSA's ability to identify and prioritize risks and capability gaps is informed by the following:

1. Enterprise Risk Management

Enterprise risk management engages organizational systems and processes together to improve the quality of decision-making for managing risks that may hinder an organization's ability to achieve its objectives. Ensuring transportation security while promoting the freedom of movement of legitimate travelers and commerce is a critical counterterrorism mission assigned to TSA. This risk management approach supports TSA's ability to identify, analyze, and respond appropriately to strategic risks across the full spectrum of TSA activities.

TSA's enterprise risks convey the intent to remain vigilant while maturing its processes and capabilities to meet the demands of a dynamic threat environment. TSA has identified and assessed its enterprise risks, which are used to inform TSA's capital investments and capability enhancements:

- Airport Screening
- Transportation Systems Sector Cybersecurity
- Insider Threats
- Emerging and Evolving Threats
- Enterprise Data Management
- Surface Transportation Security
- Workforce Retention
- TSA Cybersecurity (Internal)

2. Transportation Sector Security Risk Assessment (TSSRA)

TSSRA is an enterprise-level, cross-modal assessment that evaluates high-level attack scenarios to produce a comprehensive comparative risk landscape across all TSA mission areas. For each scenario, TSSRA uses modeling and subject matter expert input to assess threat, vulnerability,

and consequences, while considering adversary intent and capability, countermeasures and their effectiveness, and the potential human, economic, and mission impacts of successful attacks.

3. Risk and Trade Space Portfolio Analysis (RTSPA)

RTSPA provides TSA with a detailed assessment of TSA's main security systems in domestic passenger aviation, including vetting, checkpoint, and checked baggage security capabilities. RTSPA's detailed scenarios include specific intelligence-driven adversaries, threat materials, tactics, pathways, and concealments. It uses detailed laboratory and covert-testing results as inputs, and intelligence community elicitations on adversary characteristics and preferences. It identifies and prioritizes system vulnerabilities, informs strategic, data-driven decisions, and determines impacts of potential system enhancements against emerging threats. RTSPA is a key input for policy and procedural decisions, equipment characteristic and allocation decisions, the Transportation Security Capability Analysis Process (TSCAP), and the Planning, Programming, Budgeting, Execution, and Strategy (PPBE-S) processes.

4. International Risk Framework (IRF)

The IRF evaluates the relative risk of a terrorist attack onboard an international flight inbounds to the United States from a last-point-of-departure (LPD) airport. The IRF evaluates the risk components of a threat, vulnerability, and consequence at each LPD, such as an LPD's U.S. inbound flight data, countermeasure effectiveness, implementation effectiveness, known or suspected terrorist traffic, and corruption and threat information. These assessments inform policy decisions and allocation of inspection and assistance resources.

5. Transportation Security Capability Analysis Process (TSCAP)

TSCAP captures mission-essential capability needs, evaluates current performance against those needs, prioritizes capability gaps, and analyzes potential courses of action for closing the gaps. TSCAP supports the DHS Joint Requirements Integration and Management System process for obtaining DHS validation of TSA's mission need, associated capability gaps, and the recommended course(s) of action. The DHS validation provides significant support to TSA in justifying investments. Thus, TSCAP's conducted analysis rigor is critical in supporting TSA's decisions to pursue material or nonmaterial solutions, providing key inputs to TSA's PPBE-S process.

After threats, risks, and capability gaps and needs are identified and prioritized, TSA's Capability Managers (CM) lead efforts to address needs, and direct the execution of capability analysis, requirements generation and management, and capability sustainment across TSA. CMs support the following capabilities, consistent with the CIP focus areas and the capital investment/capabilities:

a. Identity Management and Vetting:

Identity Management (IDM): Ensuring the effective and efficient integration of identity-related activities and prioritization of resources including enrollment, identity proofing, vetting, and verification processes throughout the enterprise.

b. Threat Detection System-of-Systems (SoS)

Accessible Property Screening (APS): Enhancing the security effectiveness and operational efficiency of TSA's APS through automation, integration, and connection.

Alarm Resolution (AR): Advancing materiel and nonmaterial capabilities to identify, analyze, and resolve alarms accurately within the TSA security ecosystem.

On-Person Screening (OPS): Improving TSA's OPS capabilities, including Advanced Imaging Technology (AIT), walk-through metal detectors, pat-down procedures, and other emerging capabilities.

Checked Baggage: Advancing effective and efficient materiel and nonmaterial solutions in the checked baggage space.

Multimodal and Public Area Capabilities: Providing security technology recommendations and solutions for air cargo, public transportation areas, and critical infrastructure (for example, pipelines) by evaluating existing security technologies, developing requirements for new technologies, by consulting industry, by partnering with national labs and cybersecurity researchers and vendors to develop assessment tools, and stimulating the technology marketplace.

Countering Unmanned Aircraft System (C-UAS): Coordinating with the DHS Science and Technology Directorate (S&T) and the Federal Aviation Administration in the execution of capability analysis, requirements generation and management, capability and technology assessments, and capability sustainment for UAS/C-UAS across TSA.

c. Enhanced and Secure IT Systems

Field Information System (FIS): Collaborating with field security operations stakeholders to innovate and advance FIS that support security information-gathering and information-sharing among DHS, TSA, law enforcement, and intelligence community stakeholders. TSA will continue to expand the support system of CMs and will institutionalize capability management within TSA. This should ensure better coordination between CMs, TSA stakeholders, interagency partners, and industry vendors.

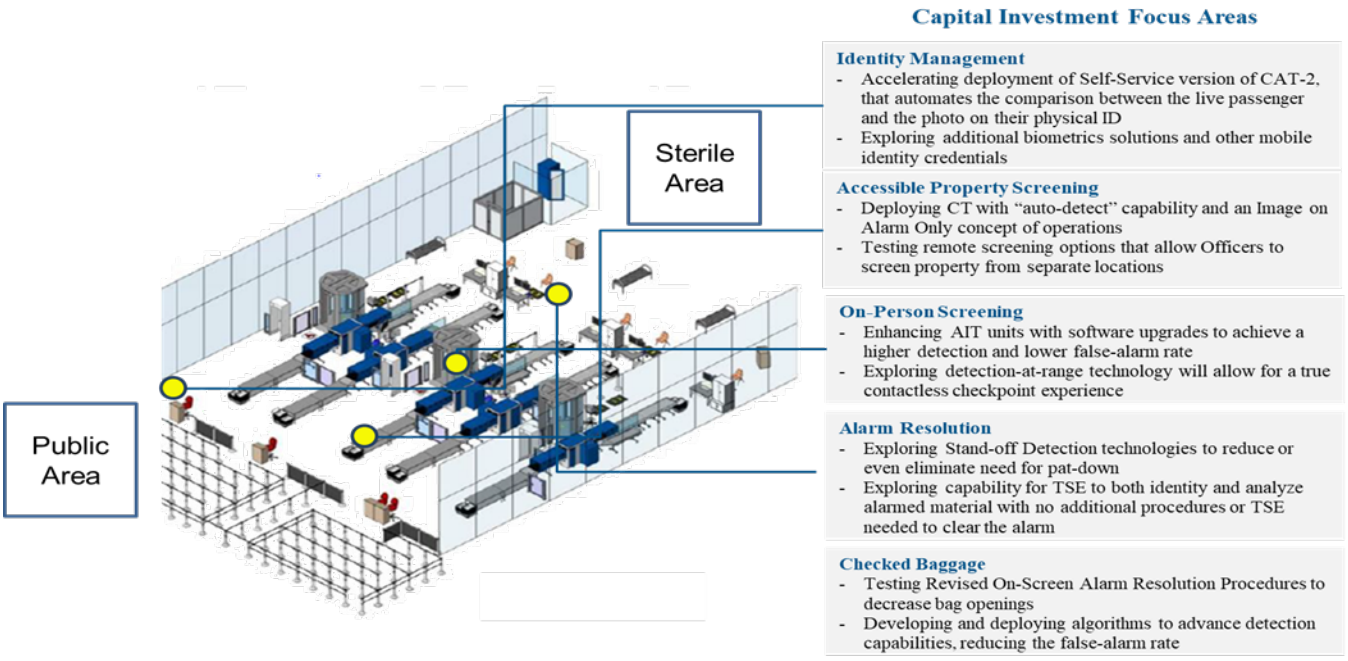
B. Transforming Mission Execution

The Nation's transportation critical infrastructure, including airports, railroads, mass transit, highway and motor carriers, pipelines, and ports must be protected from international and domestic terrorists, Nation States, criminal and other malicious cyber actors, insider threats, and other adversaries in a continually evolving transportation ecosystem. To help protect the Nation's diverse transportation assets from these varied threats, TSA must adapt to change and transform mission execution to raise the baseline for effective and efficient security, modernize IT, invest in its workforce, and improve the customer experience. To transform mission execution, TSA creates a security infrastructure comprised of capital investments and complementary policies, processes and strategic partnerships that collectively optimize security solutions, advance TSA's priorities, and strengthen transportation security.

To meet those needs, in combination with supporting policies, processes, and partnerships, TSA focuses on technologies that increase detection capability and reduce false alarm rates. Such advancements reduce the need for secondary screening that result in high contact rates between Transportation Security Officers (TSO) and passengers.

For example, TSA is leveraging Credential Authentication Technology (CAT), deploying checkpoint Computed Tomography (CT) with "auto-detect" capability and an 'Image on Alarm Only' concept of operations, and integrating advanced detection algorithms into the OPS equipment capabilities. **Figure 6** depicts how these investments and others within the airport environment are creating checkpoints of the future.

Figure 6: Capital Investment/Capability Focus Areas within the Airport Environment



Investments used to execute and transform the mission are spread across the following mission areas: 1) IDM and Biometrics, 2) Threat Detection SoS, and 3) Enhanced and Secure IT Systems. To advance these pillars, TSA plans its investments in accordance with the budget environment to establish achievable goals and objectives for each capability area, technology, and program.

To maximize the capabilities of checkpoint technologies, TSA also is investing in:

- Open Architecture (OA) implementation and associated vendor solutions to include cybersecurity;
- Plans for checkpoint security and algorithm updates, including analysis on throughput times, and time to deploy screening technologies; and
- Mitigating the risk of TSE to exposure to cyber and information attacks, which could impact checkpoint security operations.

C. TSA's Current State

TSA addresses ever-present threats to aviation, but also focuses on dynamic and emerging cybersecurity threats to our Nation's aviation, rail, mass transit, and oil and gas pipeline infrastructure. Yet even as the threats have multiplied and diversified, TSA's fundamental mission to protect the Nation's transportation systems and ensure freedom of movement for people and commerce has not changed. TSA works collaboratively with its partners to provide agile and responsive security across all modes of transportation through passenger and cargo screening; vetting and credentialing personnel in critical transportation sectors; law enforcement; regulatory compliance; and international cooperation.

This breadth of TSA activities demands a continued investment in, and acquiring and fielding of, new technologies to strengthen transportation security, remain ahead of evolving threats, hire and retain cybersecurity professionals, and maintain flexibility with the evolving nature of the transportation system.

D. Defining an Ideal Future State

TSA has begun establishing an OA environment through the Checkpoint Automation initiative to provide the ability to rapidly field screening solutions, designing an approach where manufacturers of IT system components, such as software and hardware, are standards-based and designed to be interoperable to allow a wide range of manufacturers and users (i.e., industry partners) to create improved plug and play subcomponents (for example, new detection algorithms, user interfaces, and reporting systems). In support of TSA's OA objectives, TSA published the OA Roadmap in July 2023, which serves as a foundation for providing TSA's vision, goals, and objectives to establish a connected transportation security SoS, using OA guiding principles. The Roadmap aligns and communicates TSA's OA activities, identifying short-term (within 3 years) and long-term (more than 3 years) needs to sustain success. It

informs the development and management of other strategic plans, roadmaps and implementation plans across the TSA enterprise.

In accordance with EO 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 2023), TSA collaborated with its industry stakeholders to identify AI risk and use cases. This initial effort aimed at further understanding the impacts of AI pertaining to regulatory responsibilities, governance, acquisitions, and other program elements, will inform future procurement, and investment in TSE.

Although TSA continues to maintain and update TSE, TSA must procure and deploy TSE at a faster rate than what current resources permit. The acquisition process enables flexibility and adaptability and utilizing the acquisition governance process remains critical to ensuring TSA meets its TSE deployment targets. This flexibility and adaptability ensures TSA is able to increase procurements and deployments if or when the resources become available. Currently, TSA is identifying opportunities to replace older TSE with Computed Tomography (CT) X-Rays and AITs to increase the efficiency and effectiveness of airport checkpoints. Fully funded capabilities would positively impact their full operational capability (FOC) timelines and give TSA flexibility to deploy and procure TSE.

E. Research and Development

TSA benefits from R&D work supported by DHS S&T, U.S. Department of Energy, U.S. Department of Defense, U.S. Department of Justice, and other Federal departments and agencies. TSA coordinates relevant R&D activities across these federal security experts to eliminate duplication and to maximize the adoption of applicable technologies. As an operational security agency with limited R&D funds, TSA focuses those funds on capability developments of risk-based enhancements having the greatest mission impact across people, processes, and technology.

F. Partnerships

As one of TSA's three focus areas in the Administrator's Intent 3.0, TSA collaborates with academia, industry, Federal Government, and international partners to identify and integrate technology and to process advancements into existing security systems that enhance security effectiveness and improve operational efficiency. Through working partnerships with vendors of security systems, airports, and airlines, TSA continues to identify emerging technologies that improve security, the passenger experience, and efficiency, as well as collaborative efforts to enhance innovation and research and development. Examples of these initiatives are detailed below.

1. Cybersecurity

Collaboration and coordination with cybersecurity industry stakeholders (e.g., manufacturers, vendors, governments, academia, etc.,) grows each year and becomes more crucial as cybersecurity threats evolve. TSA representatives from across the enterprise, including the Administrator, attend a Black Hat cyber and information security event, which provides the security community with cutting-edge research, development, and trends. In addition, TSA participates in DEF CON, the world's longest-running hacker event, joining a large group of security, policy, science, and technology professionals in a collaborative environment. TSA also attends the Consumer Electronics Show, which presents the latest in digital health, automotive, and smart technology. TSA's participation in these events provides invaluable opportunities to connect and collaborate with cybersecurity experts across academia, researchers, vendors, and leaders in the public and private sectors. These discussions and collaboration focus on evolving threats and technology trends, allowing us to develop appropriate risk mitigation strategies that improve the cybersecurity maturity of the sector.

2. International Collaboration

TSA establishes international relationships to exchange information and to share lessons learned, both through international organizations such as the International Civil Aviation Organization, and the European Civil Aviation Commission, and through direct relationships with specific states or member groups. Open dialogue builds and enforces joint standards, to align R&D efforts, and to test emerging capabilities to improve the global security landscape. TSA also continues working with the Airports Council International - Europe and with the European Organization for Security and Avinor - the Norway civil airport authority, for OA collaboration, most recently releasing initial guidance on OA for Airport Security Systems. In addition, TSA plans to launch the One Stop Security Pilot between March 2024-March 2025 with the United Kingdom, to include London-Heathrow airport and Jackson-Hartsfield and Dallas-Fort Worth airports. Five additional pilot locations will be chosen in accordance with commensurate screening standards.

3. Expanding and Integrating Risk-Based Security

TSA's screening process has evolved from a post 9/11 one-size-fits-all security approach to an intelligence-driven, risk-based strategy. TSA risk-based security practices expedite screening for known and trusted travelers at security checkpoints while focusing resources on high-risk and unknown passengers. TSA's security measures begin with vetting travelers against government watchlists to ensure that passengers, accessible property, and checked baggage are screened at the appropriate level. This requires collaboration with U.S. Government partners and agencies, specifically the Federal Bureau of Investigation-led Terrorist Screening Center. Security measures can be tailored more to the specific individual with more information about the traveling public via expanded TSA PreCheck® enrollment. TSA can screen travelers through

TSA PreCheck®[6] lanes at a rate of about 240 per hour, compared to 140 to 150 travelers per hour at standard screening lanes.

4. Support Threat Signature Characterization

TSA partners with external stakeholders to develop reliable, cost-effective system components (both hardware and algorithms) that meet system goals. TSA continues working with vendors, academia, national laboratories, and interagency partners to develop advanced algorithms that enhance performance of TSE including Advanced Technology (AT) and CT X-ray, Explosives Detection System (EDS), and AIT. These new algorithms use machine-learning approaches to discriminate between threats and benign objects, making the screening process more effective and efficient. TSA anticipates that machine learning algorithms not only will improve security effectiveness, but also will support automation in future security systems and reduce false alarm rates. This will enhance operational efficiency further and improve the customer experience.

TSA's Innovation Task Force (ITF) is a collaboration among TSA, manufacturers, and airports to demonstrate emerging capabilities that can drive technological, software, automated, ergonomic, environmental, or aesthetic advancements to the transportation security ecosystem. The ITF provides an avenue to work with industry to demonstrate flexible, mature, and standardized "curb-to-gate" security solutions and techniques for transportation infrastructure. Proving these solutions and techniques in an operational environment to ensures that they are viable in the intended environment. After a successful validation, TSA will consider prototypes for potential transition to requirements development, informing capability roadmaps, and, when applicable, acquisition and deployment, qualification for regulated air cargo use, or introduction as products to procure through grant programs or purchased with confidence by users nationwide.

5. Surface Security Technology

In partnership with surface transportation asset operators and industry manufacturers, the Surface Security Technology (SST) Program evaluates advanced technologies and facilitates industry awareness to help to address identified surface transportation security capability gaps. SST participates in the DHS S&T and TSA-sponsored Intermodal Transportation Research and Development Working Group, which serves as a forum for surface-based transportation operators and stakeholders to identify, discuss, and publish security capability gaps across the surface transportation sector.

G. Areas for Investment Opportunity – Unconstrained Potential Investments

TSA continues to successfully perform its mission in the current austere budget environment, but as requested communicates additional resources that would advance current capabilities. This

[6] TSA PreCheck® | Transportation Security Administration

section reflects the Agency's ability to invest in attainable technology solutions above and beyond the current President's Budget Request. These investments capture supplemental programs that have been recorded as an acquisition with dedicated funding in the programming and budgeting process, and that with the additional funding, are executable.

This section lists both active, approved procurements and capabilities that TSA could reasonably execute in the FY 2025 – FY 2029 timeline and that build on the FY 2025 President's Budget. It sets an ideal future state of TSA's capital investments and select checkpoint capabilities required to advance the security of transportation critical infrastructure and takes into account end of service capital investments that require replacement. It also contains information on additional resources that can be provided and how those resources increase new capacity and advance the timelines for FOC and replace older equipment. Having the ability to replace aging and outdated equipment in a more expedient manner gives TSA the opportunity to expand its practices to better adapt and address threats to the Nation's transportation systems.

1. IDM

In line with the FY 2025 President's Budget, roughly 75 percent of the IDM efforts are supported by fee funds and the remaining TSE procurement efforts are funded by base funding. Current IDM capabilities funded within the FY 2025 President's Budget includes Biometric Technology, CAT, and BPS. Additional funding for this capability would allow the Agency the resources to expand long-term project and capability planning to also include:

- **Mobile Driver's License (mDL) Digital Identity (DI):** Full operability requires DI R&D, which is unfunded beginning in FY 2024. This type of R&D would allow TSA to stay ahead of a rapidly changing landscape where physical ID fraud becomes more sophisticated, passengers move to digital identities, and facial recognition becomes the preferred solution for a contactless travel experience.
- **Innovation & Incubation Development:** Additional funding for innovation and technology includes enhanced networking infrastructure, faster and more secure edge devices, and Smart Phone-based mDL readers. These new technologies would allow TSA to develop and test new capabilities and enhancements to existing solutions in an agile manner.

- **REAL ID:** Support for the 2020 REAL ID Modernization Act and the resulting mDL waiver rule scheduled for publication in Summer 2024 to develop a standards-based technical governance and infrastructure that is required for state-issued mDL to be interoperable with TSA systems and accepted at TSA checkpoints.

- **DHS S&T Interagency Agreement:** Additional funding would allow TSA to better support DHS S&T on a multitude of ongoing independent, third-party testing related projects within IDM, including biometric research and development, to continue to advance the Agency's mission of securing the Nation's transportation systems. Doing so

would expand TSA's capabilities to anticipate and respond to evolving threats while encouraging resource and information sharing to advance the larger goal of Homeland Security.

The CAT program re-baselined in FY 2022 to increase the FOC quantity and to implement enhanced capabilities (CAT-2) supporting a self- service system configuration, including a camera for 1:1 facial recognition verification and authentication of mDL/digital IDs. The CAT program received DHS's approval in May 2023 to procure and deploy the CAT-2 upgrade kits that will allow for the upgrade of CAT-1 systems with CAT-2 capabilities.

As of June 2024, the fleet consists of approximately 2,054 CAT systems operating across 231 facilities (airports/training and testing centers). Of the current deployed fleet, 628 systems are CAT-1 and 1,426 are CAT-2 systems. The current budget allocates $18.9 million in FY 2025 and $96.4 million through FY 2029 for CAT. To move FOC from FY 2049 to FY 2029 for CAT-2 with a full replacement of the CAT-1 systems at the approved re-baselined amount, TSA could upgrade 368 to 388 units per year through FY 2027 which would require roughly $106 million from TSA base funding.

Within the FY 2025 budget, TSA continuously improves identity verification at checkpoints, enhances customer experience, and deploys new TSE capabilities, while buying-down risk. However, additional funding for these projects would enable TSA to accelerate these efforts while fulfilling TSE deployment goals in a shorter timeframe, without relying on older and outdated equipment.

2. Checked Property Screening System (CPSS)

TSA's current fleet of carry-on baggage screening equipment includes CT X-ray scanning known as CPSS, an enhanced imaging platform that enables the detection of a wider range of threats. TSA currently deploys roughly 777 CT units with an additional 45 piloted units across four different vendors. The FY 2025 President's Budget includes $144.7 million in FY 2025 and $731.7 million through FY 2029 for CPSS to progress towards a FY 2042 FOC with a one-for-one replacement of the legacy two-dimensional AT systems with the three-dimensional CT systems. To accelerate FOC from FY 2042 to 2029 and enhance aviation screening with new technology while avoiding the use of obsolete AT X-rays, additional funding could support the procurement of an additional 2,263 CTs above what the FY 2025-2029 funding level provides. TSA could deploy a maximum of 350 units per year due to industry production constraints and our ability to deploy equipment without disrupting checkpoint operations (refer to **Figure 7**).

Figure 7: CPSS Procurements-Current and Alternative Procurement

CPSS Procurements: Currently programmed and potential requirements					
Quantities	FY 2025	FY 2026	FY 2027	FY 2028	Total
Programmed Procurement Quantities	83	82	80	79	324
Additional Procurement Quantities	267	268	270	203	1,008
Procurement quantities are estimates and will change based on final, negotiated contract pricing and airport/operational needs in the year of execution					

The maturation of this capability would enable TSA to increase throughput and security at the nation's checkpoints by taking advantage of the automation associated with the checkpoint CT systems and improve the customer experience, as required by EO 14058.

3. AIT

AIT detects a wide range of metallic and nonmetallic threats using millimeter-wave imaging technology to screen passengers for threats that may be concealed under clothing without physical contact. Used in conjunction with Enhanced Metal Detectors (EMD), these TSE comprise TSA's On-Person Screening capability. TSA achieved FOC for AIT in 2017 with 962 units. As of Q3 FY 2024, TSA has 1,065 total AIT units deployed nationwide. In FY 2023, TSA procured 45 AIT upgrade kits, with plans to procure 18 new units with FY 2024 funding. TSA is exploring initiatives to retrofit these units to enhance detection performance, utilize software to leverage updated algorithms in accordance with OA principles, explore next-generation capabilities to increase throughput and detection, reduce false alarms and the contact rate between TSOs and passengers, and improve the customer experience.

Although FOC was achieved, additional funding would allow the Agency to expedite the required detection algorithms, retrofits, and any additional deployments for new checkpoints, further improving transportation security. To maximize AIT, additional funding ($312 million from FY 2025 to FY 2029) could be used to procure, refurbish, provide HD kits to, and deploy up to 548 units per year.

4. Checked Baggage

TSA has deployed an advanced fleet of Checked Baggage screening equipment to meet the security needs of the Nation's aviation system. EDS, which relies on CT capability, is TSA's primary capability with 1,626 currently deployed, 200 of which are near end-life. The FY 2025 budget accounts for plans to keep EDS in the field for several more decades. Any additional funds could be used for the development of a more thorough threat detection upgrade. The future of Checked Baggage at TSA places a strong emphasis on both technology and non-technology areas, with a focus on three core goals as detailed in the Capability Roadmap: detect

explosive threats, connect checked baggage to the TSA network, and effectively display threats for TSOs. To continue to expand the Agency's capability to achieve these three goals, additional investments could be directed towards advancing technology in threat detection, cyber security, and user interface. Continuous research and development to adapt and respond to changing threats, and enhancing overall baggage security effectiveness, will help develop programs to address gaps created by emerging threats.

TSA's Electronic Baggage Screening Program (EBSP) receives $250 million annually through the Aviation Security Capital Fund to comply with the 100 percent checked baggage screening mandate. The fund allows TSA to test, procure, install, sustain, and recapitalize EDS across all federalized airports. However, the Agency has identified potential opportunities for capability expansion. Up to $250 million per year (FY 2025 to FY 2029) in additional funding could support Agency's ability to pursue R&D focused on EDS enhancements, updated detection standards, solutions to false alarm reduction, improving dynamic screening, and Threat Imaging Projection.

IV. Conclusion

Despite an austere budget environment, the Transportation Systems Sector is working at all levels to maximize funding opportunities, including security improvements to aging infrastructure. Investments identified in the CIP, both in the constrained and unconstrained budget environments, are designed to position TSA to meet evolving threat challenges. The CIP provides a guide to TSA's investment approach that will advance strategic priorities while informing trade-offs between maintaining current operations and investing in, acquiring, and fielding new technologies. By considering current and future risks and threats to the transportation environment, and opportunities for collaboration with industry, the CIP helps to ensure that TSA is better equipped to identify capital requirements necessary to address identified challenges and risks to transportation security.

This investment approach directly supports TSA's dedicated professionals, ensuring that the workforce is equipped with the tools, resources, training, and infrastructure required to conduct frontline functions effectively and efficiently that mitigate risks and outmatch threats.

V. Abbreviations

Abbreviation	Definition
AAR	Advanced Alarm Resolution
ACMS	Air Cargo Management Systems
ACSTL	Air Cargo Screening Technologies List
AIP	Airport Infrastructure Protection
AIT	Advanced Imaging Technology
ALF	Acquisition Lifecycle Framework
APS	Accessible Property Screening
APSS	Accessible Property Screening System
AR	Alarm Resolution
ASL	Automated Screening Lane
AT	Advanced Technology
BLS	Bottled Liquid Scanner
BPS	Boarding Pass Scanner
CAD	Chemical Analysis Device
CAT	Credential Authentication Technology
CAT-2	Second Generation Credential Authentication Technology
CBP	U.S. Customs and Border Protection
CDC	Centers for Disease Control and Prevention
CIM	Checkpoint Information Management
CIP	Capital Investment Plan
CJ	Congressional Justification
CM	Capability Manager
COVID-19	Coronavirus Disease 2019
CPSS	Checkpoint Property Screening System
CT	Computed Tomography
C-UAS	Counter-Unmanned Aerial System
CX	Customer Experience
DHS	Department of Homeland Security
DI	Digital Identity
DICOS	Digital Imaging and Communications in Security
EBSP	Electronic Baggage Screening Program
EDC	Explosives Detection Canine
EDS	Explosive Detection System
EMD	Enhanced Metal Detector
EO	Executive Order
ePACS	Enterprise Physical Access Control System
ETD	Explosives Trace Detection
FAA	Federal Aviation Authority

Abbreviation	Definition
FAMS	Federal Air Marshal Service
FIS	Field Information Systems
FISMA	Federal Information Security Management Act
FOC	Full Operational Capability
FTE	Full-time Equivalent
FY	Fiscal Year
FYHSP	Future Years Homeland Security Program
HC	Human Capital
HD	High-Definition
HSPD	Homeland Security Presidential Directive
IAC	Indirect Air Carrier
ID	Identification Document
IDM	Identity Management
IRF	International Risk Framework
IT	Information Technology
ITF	Innovation Task Force
ITIP	Information Technology Infrastructure Program
LAX	Los Angeles International Airport
LEA	Law Enforcement Agency
LFA	Lead Federal Agency
LPD	Last Point of Departure
mDL	Mobile Driver's License
MIA	Miami International Airport
MPAC	Multimodal and Public Areas Capability
MSNS	Mission & Scheduling Notification System
NEDCTP	National Explosives Detection Canine Team Program
OA	Open Architecture
O&S	Operations and Support
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OPS	On-Person Screening
OPSL	Open Platform Software Library
OTA	Other Transactional Agreement
PACS	Physical Access Control System
PC&I	Procurement, Construction, and Improvements
Pfa	Probability of False Alarm
PFP	Personnel Futures Program
PPBE-S	Planning, Programming, Budgeting, and Execution – Strategy
PSC	Passenger Screening Canine

Abbreviation	Definition
PSP	Passenger Screening Program
R&D	Research and Development
RTSPA	Risk and Trade Space Portfolio Analysis
S&T	DHS Science and Technology Directorate
SoS	System of Systems
SRT	Security Related Technology
SST	Surface Security Technology
SSTA	Staffing, Scheduling, Time, and Attendance
STIP	Security Technology Integration Program
STSTAC	Surface Transportation Security Advisory Committee
TDC	Travel Document Checker
TSA	Transportation Security Administration
TSAAM	TSA Acquisition Manual
TSCAP	Transportation Security Capability Analysis Process
TSE	Transportation Security Equipment
TSO	Transportation Security Officer
TSS	Transportation Sector Security
TSSRA	Transportation Sector Security Risk Assessment
UAS	Unmanned Aerial System
VCS	Vetting and Credentialing System
WTMD	Walk Through Metal Detector

VI. Appendix A: Capital Investment Programs

A. Identity Management and Vetting Capability and Program Description

TSA approaches Identity Management (IDM) functions – enrollment and reservation, identity proofing, vetting, and identity verification – as a holistic lifecycle. IDM ensures the right people have access to the right transportation areas at the right time. TSA is responsible for verifying over 2.5 million identities of the traveling public per day, making it the largest identity verification provider in the United States. This ensures that individuals and passengers are vetted and properly identified prior to being granted access to the Nation's transportation infrastructure and airport sterile areas or boarding an aircraft.

Vetting

Vetting determines whether an applicant or passenger may receive a credential or access to travel based on security and/or eligibility requirements. TSA defines vetting as the process by which data provided by passengers and credentialed populations is run through the appropriate checks to determine whether a credential or access can be granted based on established authorities and guidelines governing TSA's operations. TSA vets passengers and credential holders through a combination of criminal history and terrorism checks, depending on the level of access needed. TSA's vetting capabilities are comprised of 1) a Vetting and Credentialing System (VCS), and 2) the Secure Flight Program.

Vetting	1) VCS
TSA's VCS is made up of advanced enrollment, vetting, and credentialing technology applications and is used to process Security Threat Assessments in support of TSA's credentialing programs, such as TSA PreCheck® and the Transportation Worker Identification Credential programs, among others.	

CIP Funding Levels VCS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$80.4	$80.7	$81.0	$81.3	$81.5	**$404.9**

Vetting	2) Secure Flight Program
TSA's Secure Flight Program identifies high- and low-risk passengers in order to mitigate threats to aviation security and designates travelers for enhanced screening, expedited screening, or prohibition from boarding a covered flight. The secure flight system matches commercial aircraft passengers against the Federal Bureau of Investigation's (FBI) Terrorist Screening Database, certain TSA-created watch lists, and the Centers for Disease Control and Prevention's no-fly list of individuals not permitted to travel because of disease contagion.	

CIP Funding Levels Secure Flight (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$146.4	$153.7	$157.6	$160.7	$163.8	**$782.2**

TSA is committed to consolidating the suite of technology applications that make up its VCS and reducing system duplications and will need continued funding to do so. By investing in VCS consolidations, future operating costs will be reduced and existing infrastructure will be better utilized, which creates efficiencies. TSA is equally committed to focusing its resources on the highest risk passengers and will need continued funding to refine its watch list matching, improve its vetting capabilities, expand Secure Flight to new aviation populations and data sets, increase its efficiencies and intelligence capabilities, and incorporate additional risk factors beyond its direct watch list and trusted traveler matching. These changes will improve high-risk passenger rules and watch-list matches, while decreasing false positives and minimizing the risk for potential false negatives, and more thoroughly refine passenger risk.

IDM

TSA's IDM capabilities are comprised of the following transportation security equipment (TSE) solutions: 1) Biometric Technology, 2) Credential Authentication Technology (CAT), and 3) Boarding Pass Scanners (BPS).

IDM	1) Biometric Technology
TSA's biometric technology enables verification of a passenger's identity via the comparison of a live passenger image to a verified passenger image (1:1 facial verification) or to a gallery of consenting trusted travelers (1:n facial identification). It consists of facial recognition biometric technology equipment and systems in place today, such as TSA's Second-Generation Credential Authentication Technology (CAT-2).	

CIP Funding Levels Biometrics (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$2.3	$3.5	$3.5	$3.5	$3.6	**$16.4**

IDM	2) CAT
TSA's CAT accurately verifies passenger identification documents (ID), flight reservations and prescreening status in near real-time, addressing vulnerabilities associated with ID and boarding pass fraud. CAT is connected to Secure Flight, TSA's risk-based passenger prescreening program that enhances security by matching passenger names against trusted traveler lists and watch lists. CAT authenticates acceptable forms of IDs and compares a passenger's biographic information contained on the ID to information submitted to Secure Flight during the flight reservation process. The integration of this information permits TSA to confirm a passenger has the appropriate flight reservation to proceed through security screening without having to present a boarding pass in most instances.	

TSA is upgrading CAT machines with biometric and self-service capabilities in response to Coronavirus Disease-2019. In addition to these system upgrades, biometrically enabled CAT-2 includes an updated facial-matching algorithm, software, and hardware upgrades to enhance identity verification processes.

CAT Units Deployed Across 227 Airports		
CAT	CAT-2*	Total
1,602	452	**2,054**
*CAT-2 machines are self-service configured, include a camera for 1:1 facial recognition verification, and authentic mobile driver's license and digital IDs		

CIP Funding Levels CAT (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
(O&S) $9.6	(O&S) $10.6	(O&S) $12.5	(O&S) $13.8	(O&S) $14.0	(O&S) $60.5
(PC&I) $9.3	(PC&I) $8.4	(PC&I) $6.8	(PC&I) $5.7	(PC&I) $5.7	(PC&I) $35.9
$18.9	$19.0	$19.3	$19.5	$19.7	**$96.4**

IDM	3) Boarding Pass Scanner (BPS)
TSA's BPS reads a passenger's boarding pass and displays their name, flight information, and screening status. BPS reads mobile, web-printed, and ticket counter- and kiosk-issued boarding passes. They also validate a person's TSA PreCheck® status and help Transportation Security Officers (TSO) route passengers to their appropriate screening checkpoint.	

CIP Funding Levels BPS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$0.9	$0.9	$0.9	$0.9	$0.9	**$4.5**

TSA is committed to advancing its IDM capabilities and improving the customer experience while enhancing security effectiveness and will need continued funding to do so. By investing in biometric technology, TSA can advance identity verification through facial recognition and digital identity, reduce points of contact for travelers, and pave the way for a more seamless travel experience, all while protecting a passenger's privacy and civil liberties. TSA is also committed to full REAL ID Act enforcement and will use resources provided to further upgrade its CAT systems to CAT-2 capable machines able to verify a driver's license as REAL ID-compliant. BPS will eventually be incorporated into CAT-2, allowing for a more efficient identity authentication process. Sustained funding for BPS will ensure it remains an integral part of the checkpoint identity management process until CAT systems are upgraded and CAT-2

machines are deployed to every lane at every federalized airport. TSA is committed to the integration of identity-related activities and will prioritize resources appropriated across TSA through a united strategy that enhances vetting and identity management of populations throughout the aviation security enterprise.

B. Equipment and Capability Images Catalogue

CAT	
	• Verifies passenger IDs at airport security screening checkpoints and detects and alerts the TSO to any ID that appears to be fraudulent and/or expired. • Future State: The CAT program plans to reach approval to procure and deploy the production CAT-2 system during the third quarter of FY 2024 after a favorable operational test and an acquisition decision event. The future of CAT includes upgrading the system to verify a driver's license as REAL ID-compliant to support full REAL ID Act enforcement, which takes effect on May 7, 2025.

Boarding Pass Scanner	
	• Reads a passenger's boarding pass and display the passenger's name, flight information, and risk status to the Travel Document Checker. In the case of unavailability of CAT, TSOs can use the mDL reader (which can read QR and bar codes) already on the CAT-2 to read boarding passes. • Future State: As a technology in sustainment, Boarding Pass Scanners will continue to be an integral part of the checkpoint identity management process until the CAT systems are deployed to every lane at every federalized airport. Eventually, BPS will be incorporated into CAT-2 allowing for a more efficient identify authentication process. The BPS is also the alternative identity management screening system when CAT is unavailable for use.

C. Threat Detection System-of-Systems Capability and Program Description

Checked Baggage

Managing the Checked Baggage[7] capability is critical to TSA's mission. Doing so ensures the safety of the traveling public on all commercial flights, both domestic and international. 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. TSA screens approximately 1.4 million checked bags per day for explosive materials and other threats. TSA has deployed an advanced fleet of Checked Baggage screening equipment to meet the security needs of the Nation's aviation system. The explosive detection system (EDS), which relies on the computed tomography (CT) capability, is TSA's primary capability. TSA plans to keep EDS in the field for several more decades, as additional funds are required for development of threat detection upgrades. Sufficient Operations & Support funding is required to develop new hardware and software, which allows for the test, procure, install, sustain, and recapitalization efforts.

Checked Baggage	1) EDS
TSA's EDS conducts sophisticated analysis of each checked bag. EDS captures an image of a single bag and determines if it contains a potential threat item. Type 1 EDS are multi-unit systems integrated into an airport's in-line baggage handling system, capable of screening more than 400 bags per hour. Type 2 EDS are smaller, stand-alone units usually deployed at airports with space constraints or lower screening throughput requirements. They are capable of screening up to 400 bags per hour.	

EDS Units Deployed		
EDS	EDS (End of life*)	Total
1,426	200	**1,626**
*200 units are at their end-of-life and are in the process of being recapitalized		

CIP Funding Levels Electronic Baggage Screening Program (EBSP) (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
(O&S) $282.9	(O&S) $287.5	(O&S) $292.1	(O&S) $296.7	(O&S) $301.5	(O&S) $1,460.7
(ASCF) $250.0	(ASCF) $250.0	(ASCF) $250.0	(ASCF) $250.0	(ASCF) 250.0	(ASCF) $1,250.0
$532.9	$537.5	$542.1	$546.7	$551.5	**$2,710.8**

TSA is committed to maturing its Checked Baggage capability and improving the experience of its TSOs who use the technology. Under the Aviation Security Capital Fund, which Congress established in 2004, TSA's EBSP receives $250 million annually to comply with the 100% checked baggage screening mandate. The fund allows TSA to test, procure, install, sustain, and

[7] 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.

recapitalize EDS across all federalized airports. Continued, and increased, investment in TSA's EBSP will allow TSA to 1) develop operational and functional requirements for next generation EDS machines, 2) leverage Information Technology (IT) systems to allow for near real-time data capture and storage, networked to the TSA IT Enterprise, and 3) apply an Open Architecture concept that will simplify the procurement process for EDS and support third party advanced algorithm development.

Accessible Property Screening (APS)

TSA is mandated by law to screen air travelers and their carry-on bags to identify and intercept prohibited items at the Security Screening Checkpoints at federalized airports across the United States. Screening a passenger's belongings and carry-on baggage is called Accessible Property Screening. TSA's APS capabilities are comprised of the following TSE solutions: 1) the Checkpoint Property Screening System (CPSS) program, and 2) Advanced Technology (AT) X-rays.

APS	1) CPSS
TSA's current generation of carry-on baggage screening includes CT X-ray scanning and peripheral equipment known as CPSS. CT technology automates threat detection by eliminating the variability introduced by human screeners and enables stronger detection by providing three dimensional (3D), high-resolution, X-ray images for automated threat recognition algorithms. The deployment of these CT systems provides an enhanced imaging platform for screening carry-on bags and other accessible property at security checkpoints and enables the detection of a broader range of threats. CT's enhanced imaging capabilities eliminates the need to remove electronics, laptops, and Liquids, Gels, and Aerosols from carry-on bags, improving the customer experience.	

CPSS CT Units			
Deployed	Piloted*	Donations/Demos	Total
777	45	44	**866**
*TSA currently operates 45 pilot CT units across four vendors to develop and demonstrate new capabilities developed under APS.			

CIP Funding Levels CPSS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025– 2029 Total
(O&S) $55.1	(O&S) $56.0	(O&S) $56.9	(O&S) $57.8	(O&S) $58.7	(O&S) $284.5
(PC&I) $89.6	(PC&I) $89.4	(PC&I) $89.4	(PC&I) $89.4	(PC&I) $89.4	(PC&I) $447.2
$144.7	$145.4	$146.3	$147.2	$148.1	**$731.7**

APS	2) AT X rays
TSA's AT X-ray systems screen carry-on baggage, providing threat detection capabilities for a wide range of threats by displaying dual views. TSA's existing AT X-ray systems help	

mitigate checkpoint security vulnerabilities, improve checkpoint efficiency and throughput, and reduce the number of misdirected bags identified for additional screening. AT X-rays still provide the preponderance of carry-on baggage screening across the United States.

CIP Funding Levels AT (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$72.7	$73.9	$75.1	$76.3	$77.5	**$375.5**

TSA is committed to advancing its APS capabilities and improving the customer experience while enhancing security effectiveness and will need continued funding to do so. As TSA deploys more CPSS units, it will incrementally phase out its legacy AT X-ray equipment. At current CPSS funding levels, AT X-rays are expected to remain in airports until FY 2041 and beyond. Sustained funding for AT X-rays will ensure they remain an integral part of the APS capability until CT machines are deployed to every lane at every federalized airport. By investing in CT technology, TSA can pursue advancements in both explosives and prohibited items algorithm development, "View on Alarm Only" concepts of operations, and mature its remote screening at the checkpoint, a capability that will relocate TSOs from checkpoint lanes to a remote location, thus optimizing staffing potential, improving operational efficiency, and distancing TSOs from the traveling public for increased health safety.

On-Person Screening (OPS)

TSA's OPS capability ensures the safety of commercial aviation by screening air travelers and aviation workers entering the sterile area of the airport. OPS is charged with identifying and intercepting prohibited items carried on persons through the Security Screening Checkpoints of federalized airports across the United States. TSA's OPS capabilities are comprised of the following TSE solutions: 1) Advanced Imaging Technology (AIT), and 2) Walk-Through Metal Detectors (WTMD).

OPS	1) AIT
TSA's AIT detects a wide range of metallic and nonmetallic threats using millimeter-wave imaging technology to safely screen passengers for threats that may be concealed under clothing without physical contact. AIT are able to detect a broad spectrum of materials concealed on an individual within milliseconds, speeding checkpoint-screening operations and increasing throughput.	

AIT Units		
Deployed	Procured*	Planned Deployment in FY 2024*
1,065	0	6
* FY 2023 TSA procured 45 AIT upgrade kits, with funding requested to procure 18 units in FY 2024.		

CIP Funding Levels AIT (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total

$42.9	$43.5	$44.1	$44.7	$45.4	$220.6
*Includes On-Person Detection/Next Gen AIT					

OPS	2) WTMD
TSA's WTMD is used for passenger screening. WTMD's are a type of Enhanced Metal Detector (EMD). EMDs are used to detect potentially dangerous metallic threats to aviation security. They allow for the rapid inspection of passengers in transit, while maintaining compliance with strict standard security requirements. EMDs provide a screening method for travelers enrolled in one of the DHS Trusted Traveler Programs and for those persons unable to complete AIT screening. EMDs are also used at airports where a checkpoint lane does not have an AIT, and in conjunction with an AIT to maintain throughput when the AIT cannot handle the passenger traffic presented at the lane.	

EMD Units Deployed
Total
1,401

CIP Funding Levels WTMD (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$3.3	$3.4	$3.5	$3.6	$3.7	$17.5
*WTMD are part of the Passenger Screening Program Legacy					

TSA is committed to establishing the Next-Generation OPS Program while maintaining its current program fleet aimed at increasing throughput, enhancing detections standards, and eliminating checkpoint bottlenecks associated with passenger screening. For nearly a decade, AIT systems have been deployed at Security Screening Checkpoints and they will remain key components of passenger screening. TSA intends to use existing funds to extend the current AIT fleet's useful life by developing, certifying, and procuring high-definition AIT Wideband kits with updated software that will improve detection and allow TSA to leverage third-party algorithms. TSA will also invest in field testing and deploying a cybersecurity-enhanced, Secure Technology Integrated Program (STIP)-connectable software package in reaching 100% gender neutrality across the entire AIT fleet. TSA's AIT and EMD systems will continue to provide primary and secondary screening capabilities for the checkpoint, while new Next-Generation technologies are being developed to detect more threats with fewer false alarms, move people through the checkpoint seamlessly, display information consistently across checkpoint technologies, and increase secure network connectivity. TSA will continue to pursue and invest in R&D for Next-Generation OPS program technologies that can achieve screening at speed, discriminate between different materials, and scan footwear on passengers.

Alarm Resolution (AR)

At TSA, when Checked Baggage, Accessible Property, or On-Person primary screening devices detects a potential threat, an alarm is generated. TSA's AR capability uses secondary screening

countermeasures to determine whether the person or property can be allowed into the secure area of the airport. These countermeasures consist of both AR and Advanced Alarm Resolution (AAR) operations, which seek to effectively identify, analyze, verify, and resolve alarms from primary screening. Where possible, TSA empowers TSOs to use AR countermeasures to clearly verify the alarmed material as benign or a threat without requiring further AAR procedures or devices to resolve the alarm fully. AR is also focused on establishing the capability to connect TSE in order to improve data sharing, fleet maintenance, cybersecurity monitoring, and algorithm development. TSA's AR capabilities are comprised of the following TSE solutions: 1) ETD; 2) Bottled Liquid Scanner (BLS); and 3) Chemical Analysis Device (CAD).

AR	1) ETD
TSA's ETD is used to screen checked baggage, passengers, and their accessible property quickly and accurately for explosive trace from a wide range of threats on a variety of surfaces by relying on ion mobility spectrometry technology. ETD is TSA's most relied-upon AR capability. 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. ETD detects explosive threats concealed in checked baggage and is used primarily in operations as a secondary screening resolution tool for EDS alarms, except at smaller airports, where it is used for primary screening of checked baggage. ETD units are also used to test carry-on bags that have alarmed at an AT X-ray machine. Finally, ETD detects explosive threats on passengers and/or concealed in carry-on baggage by providing a means for operators to examine articles for explosives residue on passengers and bags.	

ETD Units Deployed
Total
5,874

CIP Funding Levels ETD (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$49.5	$50.3	$51.1	$51.9	$52.8	$255.6

AR	2) BLS
TSA's BLS differentiate dangerous liquids and compounds from common, benign substances carried by passengers. BLS aids TSA in identifying explosive, flammable, or hazardous substances that have been concealed in a benign container. The containers do not have to be open for the analysis to be performed. Using Raman Spectroscopy (laser) and electromagnetic technology, BLS units quickly analyze and identify the chemical compositions of a wide variety of solids and liquids, including explosives that are currently on the classified threat list.	

BLS Units Deployed
Total
1,633

CIP Funding Levels BLS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$1.7	$1.7	$1.8	$1.8	$1.8	$8.8
*BLS is part of the Passenger Screening Program Legacy					

AR	3) CAD
TSA's CAD screens unknown liquid and solid (including powder) materials. CAD systems detect and identify threat substances concealed on individuals and their accessible property entering the sterile area of an airport terminal through the passenger screening checkpoint. They provide Transportation Security Specialist-Explosives personnel with the capability to identify unknown liquid and solid materials in the field. These can include explosives, precursors, and other materials	

CIP Funding Levels CAD (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$0.8	$0.8	$0.8	$0.8	$0.8	$4.0
*CAD is part of the Passenger Screening Program Legacy					

TSA is committed to effectively mitigating credible threats to aviation through its AR capability and taking AR from its current state to the next generation capability and will need continued funding to do so. TSA's current ETD and BLS fleets are approaching the end of their useful life and TSA intends to replace them with next generation capabilities titled Trace Resolution Technology (TRT) and Bulk Resolution Technology (BRT) respectively. Until then, periodic purchases of current ETD and BLS models are necessary to meet airport growth and required safety stock needs. In addition, TSA will acquire new CAD systems with the ability to identify unknown liquid and solid materials as part of its airport screening operations.

Multimodal and Public Area Capabilities (MPAC)

MPAC provides security technology recommendations and solutions for air cargo, public areas, and critical infrastructure by evaluating existing and developing new security technologies. TSA's MPAC capabilities consist of the following: 1) Surface Security Technology; 2) Air Cargo Management Systems (ACMS); 3) Public Areas; and 4) Critical Infrastructure.

MPAC	1) Surface Security Technology
TSA established its MPAC Surface office as a direct result of the 2004 and 2005 Madrid and London train and public transportation bombings. MPAC Surface leads and promotes Surface Security Technology (SST) innovation through the operation of test beds. SST test beds evaluate the operational performance and suitability of candidate technologies at hundreds of simulated real-life surface transportation environments across the United States representing all surface transportation modes.	

CIP Funding Levels SST (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$7.9	$7.9	$7.9	$7.9	$7.9	$39.5

MPAC	2) ACMS

Air cargo plays a critical role in the U.S. economy, and the security of the air cargo system is at the core of TSA's mission. Passenger airlines and all-cargo carriers are mandated by law, and changes to International Civil Aviation Organization standards, to screen 100 percent of cargo transported on their aircraft.[8] TSA's ACMS Branch is responsible for ensuring the security of cargo transported on passenger aircraft and the Air Cargo Security Technology Program. ACMS's IT systems are used by over 15,000 industry partners they vet, approximately 7.3 million shippers and 270,000 air cargo workers, and they support the regulation of over 4,000 Indirect Air Carriers.

CIP Funding Levels ACMS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$10.2	$10.4	$10.6	$10.8	$11.1	$53.1

MPAC	3) Public Areas

Terrorist attacks and mass shootings, such as those that occurred at Brussels International Airport, Istanbul Ataturk Airport in Europe, and Ft. Lauderdale-Hollywood International Airport in Broward County, Florida, reinforce the need to enhance security in public areas of transportation facilities, to include airport public areas and surface transportation assets. In public areas, traditional security screening procedures that require divestment of articles from travelers and an intrusive and slow search process are unrealistic. TSA has recently undertaken efforts to analyze and test perimeter intrusion detection and deterrence technologies as part of its Airport Infrastructure Protection program and perform limited assessments of Automated Exit Lane technology.

MPAC	4) Critical Infrastructure

Critical infrastructure refers to vital systems and assets, whether physical or virtual, whose incapacity or destruction may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, of any federal, state, regional, territorial, or local jurisdiction. TSA supports the efforts of public and private critical infrastructure owners and operators to manage risks by identifying, deterring, detecting, disrupting, and preparing for threats and hazards; by reducing vulnerabilities of critical assets, systems, and networks; and by mitigating potential consequences should incidents occur.

[8] See section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. Law 110–53 (Aug. 3, 2007), codified at 49 U.S.C. 44901(g).

TSA will continue to 1) identify, test, and evaluate layered technologies for sophisticated infrastructure protection using combinations of sensors and analytics systems, and 2) make next-generation products that will better detect intrusions and other unauthorized events. In addition, TSA is particularly interested in providing prevention, timely detection and identification, situational awareness, and efficient mitigation and response to chemical and biological threats.

TSA is committed to advancing its MPAC and will need continued funding to do so. By investing in multimodal screening systems – such as primary and secondary screening technologies – across multimodal transportation infrastructure, threat detection capabilities will be enhanced. TSA's goal is to increase detection capability for known threats, to increase its ability to detect smaller threat masses, and to increase the number of advanced multimodal screening technologies. MPAC's priority investments include continued evaluation of next-generation technologies to improve security effectiveness and operational efficiency in the air cargo environment and continued support of operational test beds for different modes of transportation (mass transit, highway motor carrier, pipeline, freight rail, maritime, public areas, critical infrastructure protection, and airport perimeters).

Counter-Unmanned Aircraft Systems (C-UAS)

TSA's C-UAS capability development is led by the TSA C-UAS Capability Integration Council (CIC). The CIC utilizes an enterprise-wide integration framework, with decision-maker representation from the TSA components responsible for technology requirements and capabilities analysis, operational response and vulnerability assessment, security operations, policy, legal, budget, and information technology entities. TSA's primary C-UAS capabilities are comprised of the following: 1) the Test Bed Program 2) the C-UAS Technology Working Group, and 3) the UAS Geospatial Analysis Tool.

C UAS	1) Test Bed Program
TSA has established two UAS technology test beds at Miami International Airport (MIA) and Los Angeles International Airport (LAX). These test beds allow TSA to test selected systems to better understand the capabilities and limitations of UAS technologies in an airport environment and keep pace with the rapidly evolving technology marketplace and threats. TSA shares in-progress data summaries, technology testing results, and lessons learned with appropriate stakeholders.	

C UAS	2) C UAS Technology Working Group
TSA and FBI co-chair the C-UAS Technology Working Group, comprised of more than 30 agencies, that reports to the UAS Security Senior Steering Group and UAS Executive Committee. This group facilitates information and resource sharing across the over 30 agency working group members to establish standards, align C-UAS efforts, and develop C-UAS capabilities	

C UAS	3) Unmanned Aerial System (UAS) Geospatial Analysis Tool.
TSA has access to and is monitoring UAS detections from over 40 systems across the country and integrating the data into a UAS Geospatial Analysis Tool that organizes both historical and near-real-time UAS activity nationwide in support of increasing TSA's air domain awareness and informing resource allocation prioritization.	

CIP Funding Levels C UAS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$11.6	$11.8	$12.0	$12.1	$12.2	$59.7

TSA's C-UAS Test Bed Program has established a regular cadence for adding technologies for assessment at both the MIA and LAX test beds and is providing in-progress data summaries to relevant stakeholders. As technologies advance, TSA will add more complex technologies to the test beds using a system-of-systems (or "layered approach"). The test bed program will also incorporate UAS testing at surface test bed locations when funding is available. TSA conducted its second flight test event at LAX in April 2023, flying simulated UAS threats against 3 detect, target, intercept systems to assess their effectiveness in an operational airport environment, comprising over 100 sorties and 7 types of UAS.

Information gathered from testing these systems at C-UAS test beds will benefit thousands of critical infrastructure sites, as TSA will share testing results, best practices, and lessons learned with state, local, tribal, and territorial entities, local law enforcement, the airport authority, and over 30 government agencies through the C-UAS Technology Working Group. TSA is also developing and maintaining a UAS technology security catalogue that will be accessible to these stakeholder groups via an online portal on the Homeland Security Information Network.

National Explosives Detection Canine Team Program (NEDCTP)

At TSA, canine teams are an integral component of our strategy to protect the transportation systems sector against terrorist attacks and the use of improvised explosive devices. Bomb threats cause disruption of air, land, and sea commerce and pose an unacceptable danger to the traveling public. Explosives detection canine teams are proven and reliable resources in the detection of explosives and are a key component in a balanced counterterrorism program.

The TSA NEDCTP has trained and deployed TSA-led and state and local law enforcement (LE)-led explosives detection canine (EDC) teams in support of day-to-day activities protecting the Nation's transportation systems. However, funding in the FY 2025 budget is not available for State and local LE stipends.

NEDCTP Units Deployed		
LE-Led	TSA-Led	Total
675	428	1,103

TSA has two types of canine teams: Passenger Screening Canines (PSC) and EDCs. PSC teams are trained to detect explosives concealed on the body or artfully concealed in a passenger's accessible property while the passenger is traversing through the security checkpoint. TSA's EDC teams are partnerships between TSA and State and local LE agencies within the aviation, mass transit, and maritime sectors and trained to target stationary objects. This variance in training allows the PSC to recognize a person as a possible target, so potentially following this person is a skillset not taught to EDCs. The PSCs must also work in close proximity to people without being invasive, which takes time and effort to accomplish.

CIP Funding Levels NEDCTP (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$162.6	$164.6	$168.9	$173.3	$177.8	$847.2

TSA's EDC teams had previously partnered with State and local LE agencies within the aviation, mass transit, and maritime sectors and trained to target stationary objects.

D. Equipment and Capability Images Catalogue

Type 1 EDS: Multi unit integration with Baggage Handling System	
	• Used in in-line baggage systems, capable of screening more than 400 bags per hour (BPH). • Future State: The Checked Baggage fleet consists of approximately 1,626 EDS. Of these EDS, 198 are Smiths Detection CTX 9000 and CTX 9400 systems, as well as two CTX 5500 systems which are all end of life and in the process of being recapitalized. These recapitalizations require close coordination with airports, the replacement of in-line systems is a years-long process where TSA works with airports who manage the construction.

Type 2 EDS: Stand Alone Reduced Size EDS	
	• Usually deployed at airports with space constraints or lower screening throughput requirements, capable of screening up to 400 BPH. • Future State: The Checked Baggage fleet consists of approximately 1,626 EDS. Of these EDS, 198 are Smiths Detection CTX 9000 and CTX 9400 systems, as well as two CTX 5500 systems which are all end of life and in the process of being recapitalized. These recapitalizations require close coordination with airports, the replacement of in-line systems is a years-long process where TSA works with airports who manage the construction.

	• Enables 3D imaging platform for enhanced visual interpretation and image manipulation versus 2D X-ray imaging. • Allows upgrades to automatically detect a broader range of threats. • Future State: TSA is shifting from qualification to upgrades as it continues to procure new CT systems towards achieving FOC. TSA will plan for and conduct annual upgrade releases to be applied to the current fleet as well as subsequent new production units. Implementation of upgrades each year will stem from TSA's work with vendors to provide both new capabilities and enhancements to existing capabilities, such as Prohibited Item detection and locally networked Remote and Cross-lane Screening capability. TSA will also work with CT manufacturers to transition currently proprietary systems into systems that can accommodate an Open Architecture ecosystem envisioned by TSA.

AT X ray	
	• X-ray systems that screen carry-on baggage providing threat detection capabilities for a wide range of threats by displaying dual views. • Future State: AT technology is near end of technological capability, however AT X-rays are expected to remain in airports until at least FY 2041. TSA will continue to focus on decommissioning and partial refurbishments/ redeployments as necessary and managing any end-of-life or parts obsolescence issues that may arise in the coming years.

AIT	
	• Detects a wide range of metallic and nonmetallic threats in a matter of seconds using millimeter wave to safely screen passengers for threats (that may be concealed under clothing) without physical contact. • Future State: TSA will look to connect units to a secure network that will provide for automated metrics connection to enhance data accuracy and availability, and detection performance.

EMD	
	• Detects potentially dangerous metallic threats to aviation security. EMDs provide a screening method for travelers enrolled in one of the DHS Trusted Traveler Programs and for those persons unable to complete AIT screening. The EMD also is used at airports where a checkpoint lane does not have an AIT, and in conjunction with an AIT to maintain throughput when the AIT cannot handle the passenger traffic presented at the lane. • Future State: EMDs will continue to provide primary and secondary screening capabilities for the checkpoint while new technologies are being developed to better detect ever-evolving threats.

ETD	
	• Detects explosive threats on passengers and/or concealed in carry-on baggage. ETD provides a means for operators to examine articles for explosives residue on passengers and bags. • Future State: A next generation capability called Trace Resolution Technology (TRT) is required to detect emerging threats and to replace the current legacy fleet, which is approaching end of life.

BLS	
	• Differentiates dangerous liquids and compounds from common, benign substances carried by passengers. • Future State: A next generation replacement capability, BRT, will be required to meet new detection standards and to accommodate additional bottle types.

CAD	
	• Screens unknown liquid and solid (including powder) materials. • Future State: New CAD systems will provide Transportation Security Specialist Explosives (TSS-E) personnel with the ability to identify unknown liquid and solid materials as part of airport checkpoint screening operations.

E. Enhanced and Secure IT Systems Capability and Program Description

Information Technology Infrastructure Program (ITIP)

The TSA ITIP is comprised of 34 systems that provide secure and reliable IT and communications products, services, solutions, support, and sustainment of IT services to all TSA federal employees, contractors, and support personnel. ITIP manages the 24x7x365 operations, maintenance, and service of the IT infrastructure to ensure uninterrupted operational availability of IT services required for all business and mission needs. ITIP executes a delivery model that effectively meets TSA's service level requirements while providing: technical support and enhancements, administration, project management, engineering design and implementation, and deployment services. ITIP's cybersecurity support activities include: monitoring network for vulnerabilities; mitigation or remediation actions associated with security incidents; and responding to active threats/intrusions into TSA systems. ITIP infrastructure includes computer networking, and communications capabilities in data centers and various cloud environments.

CIP Funding Levels ITIP (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$390.2	$396.8	$403.7	$410.7	$417.7	**$2,019.1**
*This includes funds for Cybersecurity					

TSA will place cybersecurity at the front of all capability development, ensuring ITIP solutions are secure at their foundation while reducing the time to develop, test, and deploy. Solutions will focus on the customer journey, improve customer feedback channels, and improve on ways to amplify customer voices to ensure ITIP delivers customer experience-driven solutions. ITIP will also continue to integrate and embed cybersecurity into its operations through the implementation of Zero Trust Architecture, providing flexible processes for managing security / privacy risk. TSA will prioritize modernization of existing capabilities while simultaneously transitioning them to cloud and operation and maintenance of the existing infrastructure and capabilities. Additionally, ITIP will explore the use of Robotic Process Automation and AI platforms to deliver automated Customer Experience (CX) driven solutions that can improve CX throughout TSA. ITIP will also develop and expand its use of Business Intelligence by leveraging the Enterprise Business Intelligence system for extracting data to use in reporting tools that will empower decision-makers with more robust data.

Field Information Systems (FIS)

FIS develops, integrates, and collaborates on capability roadmaps with stakeholders to develop and prioritize requirements at each stage of capability development and monitor and manage pilots to develop reporting capability readiness metrics and conduct operational assessments.

TSA collaborates with stakeholders to innovate and advance FIS that support security information gathering and information sharing among DHS, TSA, law enforcement, and intelligence community stakeholders.

FIS	1) Staffing, Scheduling, Time, and Attendance (SSTA)
SSTA streamlines airport functions with a centralized platform and workflows to address scheduling requirements and provides our officers with self-service capabilities including leave and shift trade requests. SSTA will reduce the administrative burden on airports based on current manual, paper-based processes and reduce resource requirements, allowing officers to return to more operational roles. SSTA also improves airport scheduling operations with near real-time data to determine resource needs and optimization. The SSTA program has several initiatives planned that will address schedule and resource management, additional mobile services, TSO training, maintenance of the Electronic Time, Attendance, and Scheduling System, and enhanced staffing modeling.	

CIP Funding Levels SSTA (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$18.3	$18.4	$18.5	$18.7	$18.8	**$92.7**

TSA's FIS Capability Management team is in the improvement phase of a continuous process improvement project that has identified information systems supporting a real-time process for both the Law Enforcement Officer check-in and incident response. Additionally, FIS will provide a technical solution for REAL ID implementation to reduce the risk surrounding non-compliant REAL ID travelers.

STIP

STIP provides a dynamic and adaptable communications infrastructure to facilitate the transfer of data between TSE and TSA. This automated support system enables centralized management and monitoring of TSE and provides the ability to respond to a rapidly changing threat environment in an agile manner. This results in improvements to efficiency and effectiveness of screening operations, threat detection, and risk analysis. STIP facilitates the collection and distribution of operational information from security equipment to a centralized server to perform data analytics, remote updating, and other system integrations. As of December 2023, there are 226 STIP-enabled locations (encompassing airports, Transportation Systems Integration Facility, and TSA Academy) with 2,057 STIP-enabled TSE units deployed (2054 CAT and 3 EMD units).

CIP Funding Levels STIP (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$14.9	$15.1	$15.3	$15.6	$15.8	**$76.7**

At the end of FY 2024, it is anticipated that there will be over 2,500 units of STIP-enabled TSE connected to TSA-Net. In FY 2025, an additional 573 units will be added to the network. TSA's path forward is to provide support for TSE to allow for the integration of security screening technologies, while handling communication with an accelerated number of TSE without any latency. Enhancements to the STIP platform will support new capabilities to include emerging biometrics technology, remote maintenance, and/or support of current and future cybersecurity posture without disruptions to airport operations.

Mission Scheduling Notification System (MSNS)

MSNS program enables the TSA Federal Air Marshal Service (FAMS) to deploy FAMs on flights in accordance with risk-based prioritization to protect U.S. air carriers, airports, passengers, and crews. MSNS uses an aggregate of nine system components, with a core application (Sabre Aircrews) designed explicitly for commercial airline crew management, and multiple additional systems and tools. The system is currently undergoing modernization via adaptive maintenance to deploy an itinerary planning tool via cloud services, human-centric design, data driven architecture, and shift-left security. This will result in significant cost savings by sunsetting legacy system components and services. The adaptive maintenance initiative referred to as FAMS Airline Scheduling Tool is in progress and at the development stage of transitioning into the cloud environment. The incremental approach, employing Agile methodology, aims to roll out functionality into the cloud within a 24-month period, leading to the retirement of the legacy system by 2027.

CIP Funding Levels MSNS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$20.4	$20.8	$21.1	$21.4	$21.8	**$105.5**

Enterprise Physical Access Control Systems (ePACS)

The ePACS is a system that complies with Homeland Security Presidential Directive (HSPD)-12 (Identity Verification) and allows each airport field location to confirm identity and access with the Federal Bridge. TSA must adhere to the direction of the Interagency Security Committee and its risk management processes along with the HSPD-12 and Office of Management and Budget Memorandum 19-17. These policies establish the requirement to integrate Physical Access Control Systems (PACS) into a unified enterprise system for all TSA- owned and/or -leased facilities and IT systems.

To migrate TSA facilities successfully to ePACS, the TSA Physical Security Office relies on the nationwide security contract to assess, provide upgrade installs, and provides technical support for the current security systems at more than 600 TSA facilities, and to migrate the equipment to the Field Security Network. The current contract provides support for security enhancements, service repairs, preventative maintenance, and ePACS implementation nationwide. As of December 2023, 259 of 600 facilities (43%) have PPACS installed or in progress towards completion.

CIP Funding Levels ePACS (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$10.5	$10.6	$10.8	$11.0	$11.2	**$54.1**

The ePACS program will continue upgrading security systems and migrating PACS for all TSA-owned and/or leased facilities through its partnership with DHS Office of the Chief Security Officer, industry technical experts, and other federal agencies in support of this initiative, and through the PACS Modernization Working Group Charter, which will advise TSA on emerging physical access control methods for updates within the HSPD-12 program.

Human Capital (HC) IT Modernization Personnel Futures Program (PFP)

The PFP provides end-to-end HC services, covering the entire lifecycle of the TSA employee, including recruitment, assessments, hiring, personnel, and payroll and benefits processing. TSA HC systems are undergoing the HC modernization effort to update outdated legacy systems, to maximize automation, integration between disparate systems and increase self-service capabilities to improve the end user experience.

CIP Funding Levels HC IT PFP (in millions)					
FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2025 – 2029 Total
$146.8	$152.0	$154.5	$156.9	$159.3	**$769.5**

By FY 2025, PFP is planning to deploy additional self-service capabilities that will empower employees to manage their benefits and personal elections; standing up a new Performance Management System with enhanced user functionality and integration; and building out automation between its multiple IT platforms. By FY 2026, TSA will continue the enhancement of its HC operational processes to improve customer experience

VII. Appendix B: Mandates for the Capital Investment Plan

TSA's intent for the Capital Investment Plan (CIP) is to meet the requirements of the 5-year technology investment plan (as required by section 1611 of Title XVI of the Homeland Security Act of 2002, as amended by section 220 of the FY 2024 DHS Appropriations Act (P.L 118-47) and its accompanying Joint Explanatory Statement; and by the Transportation Security Acquisition Reform Act (P.L. 113-245)). The table below shows where the requirements are discussed within the CIP.

Compliance Matrix

Requirement	Requirement Description	Report Location
b(1)	Develop 5-year technology investment plan in consultation with the Under Secretary for Management.	*Not Required for Refresh*
b(2)	Develop 5-year technology investment plan in consultation with the Under Secretary for Science and Technology.	*Not Required for Refresh*
b(3)	Develop 5-year technology investment plan in consultation with the Chief Information Officer.	*Not Required for Refresh*
b(4)	Develop 5-year technology investment plan in consultation with the aviation industry stakeholder advisory committee established by the Administrator.	*Not Required for Refresh*
d(1)	The plan shall include an analysis of transportation security risks and the associated capability gaps that would be addressed best by Security Related Technology (SRT).	II. A.
d(1)	The plan shall include consideration of the most recent Quadrennial Homeland Security Review.	Most recent Quadrennial Homeland Security Review was released in 2023
d(2)B	The set of SRT acquisition needs shall include planned technology programs and projects with defined objectives, goals, timelines, and measures.	II. B. Appendix A – Capital Investment Programs

Requirement	Requirement Description	Report Location
d(3)	The plan shall include an analysis of current and forecasted trends in domestic and international passenger travel.	I. A
d(4)	The plan shall include an identification of currently deployed SRTs that are at or near the end of their lifecycles.	Appendix A– Capital Investment Programs
d(5)	The plan shall include an identification of test, evaluation, modeling, and simulation capabilities, including target methodologies, rationales, and timelines necessary to support the acquisition of the SRTs expected to meet the needs under paragraph (2)-d(2)A and d(2)B	*Appendix A* – Capital Investment Programs
d(6)	The plan shall include identification of opportunities for public-private partnerships.	II. F
d(6)	The plan shall include identification of opportunities for small and disadvantaged company participation.	II. F
d(6)	The plan shall include identification of opportunities for intragovernment collaboration.	II. F
d(6)	The plan shall include identification of opportunities for university centers of excellence.	II. F
d(6)	The plan shall include identification of opportunities for national laboratory technology transfer.	II. E

Requirement	Requirement Description	Report Location
d(7)	The plan shall include identification of the Administration's acquisition workforce needs for the management of planned SRT acquisitions, including consideration of leveraging the acquisition expertise of other federal agencies.	II. C & D
d(8)	The plan shall include identification of security resources, including information security resources that will be required to protect SRT from physical or cyber-enabled theft, diversion, sabotage, or attack.	II. B
d(9)	The plan shall include identification of initiatives to streamline the acquisition process and to provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation.	II. C
d(10)	The plan shall include an impact assessment to commercial aviation passengers.	**NOT INCLUDED**
d(11)	The plan shall include a strategy for consulting airport management, air carrier representatives, and Federal Security Directors whenever an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with such officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations.	II. A & C
d(12)	The plan shall include an identification of SRT interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems.	II. B & D II. F.2 II. G.2

Requirement	Requirement Description	Report Location
e(1)	To the extent possible, and in a manner that is consistent with fair and equitable practices, the plan shall leverage emerging technology trends and research and development investment trends within the public and private sectors.	II. E
e(2)	The plan shall incorporate private-sector input (aviation industry, stakeholder advisory committee) through requests for information, industry days, and other innovative means consistent with the Federal Acquisition Regulations.	II. F
e(3)	The plan shall identify technologies in existence or in development that, with or without adaptation, are expected to be suitable to meeting mission needs.	II. A, B, G Appendix A – Capital Investment Programs
f	With the 5-year technology-investment plan, a list of nongovernment persons that contributed to the writing of the plan shall be provided.	*Not Required for Refresh*
g(1)	Beginning 2 years after the date the plan is submitted to Congress under subsection (a), and biennially thereafter, the Administrator shall submit to Congress — an update of the plan.	*FY 2025 – FY 2029 Capital Investment Plan*
g(2)	Beginning 2 years after the date the plan is submitted to Congress, and biennially thereafter, the Administrator shall submit to Congress - a report on the extent to which each SRT acquired by the Administration since the last issuance or update of the plan is consistent with the planned technology programs and projects identified under subsection d(2) for that SRT.	**NOT INCLUDED**

Requirement	Requirement Description	Report Location
(h)	(1) be prepared in consultation with— (B) the Surface Transportation Security Advisory Committee established under section 404…	*Reviewed by Surface Transportation Security Advisory Committee*
(h)	(2) include— (A) information relating to technology investments by the Transportation Security Administration and the private sector that the Department supports with research, development, testing, and evaluation for aviation, including air cargo, and surface transportation security…	*Transforming Mission Execution* – Research and Development
(h)	(B) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted…	*Appendix* – TSE Acquisition Update
(h)	(C) information relating to equipment of the Transportation Security Administration that is in operation after the end of the life cycle of the equipment specified by the manufacturer of the equipment…	*Appendix* – Capital Investment Programs
Advanced Integrated Passenger Screening Technologies	TSA is directed to submit a detailed report on passenger and baggage screening technologies not later than 180 days after the date of enactment of this act. The report shall include a useful description of existing and emerging technologies capable of detecting threats concealed on passengers and in baggage, as well as projected funding levels for each technology identified in the report for the next 5 fiscal years.	*Appendix A* – Capital Investment Programs