Capital Investment Plan

FY 2024–FY 2028

August 23, 2023

Fiscal 2023 Report to Congress

Homeland Security

Transportation Security Administration

Message from the Administrator

August 23, 2023

I am pleased to present the following "Capital Investment Plan" (CIP) for fiscal year (FY) 2024 – FY 2028, which was prepared by the Transportation Security Administration (TSA).

TSA compiled the CIP according to reporting requirements in the FY 2023 Department of Homeland Security (DHS) Appropriations Act (P.L. No. 117-328), 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.

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

The Honorable Kay Granger
Chairwoman, 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 will remain a top target for malicious actors, including international and domestic terrorists and state and non-state actors, especially in the cyber realm, due to the prevalence of soft targets within the sector, the public accessibility of many transportation modes, and the importance of transportation infrastructure to the Nation. TSA carefully monitors this evolving threat environment and the need to strategically manage risks. Risk-based decision-making is inherent to the TSA mission of protecting the Nation's transportation systems, to ensure the freedom of movement for people and commerce. The challenges and risks TSA encounters will only become more complex; therefore, TSA needs to position itself to be more strategic in responding to risks and in developing solutions.

Harnessing innovative technology is a major priority for DHS. While personnel are critical to the success of capital investments, the CIP for FY 2024 – FY 2028 outlines TSA's strategy for continuous and sustained investment in new, and the replacement of obsolete, TSE and other transportation security solutions. In the current constrained environment, the CIP demonstrates how TSA continues to advance its strategic priorities given the dynamic threats facing transportation security through combined investment in security solutions, policy and process improvements, and partnerships. TSA will continue to responsibly invest in, acquire, and field new technologies and enhance information technology (IT) systems, through existing contracts, to strengthen security effectiveness and efficiency.

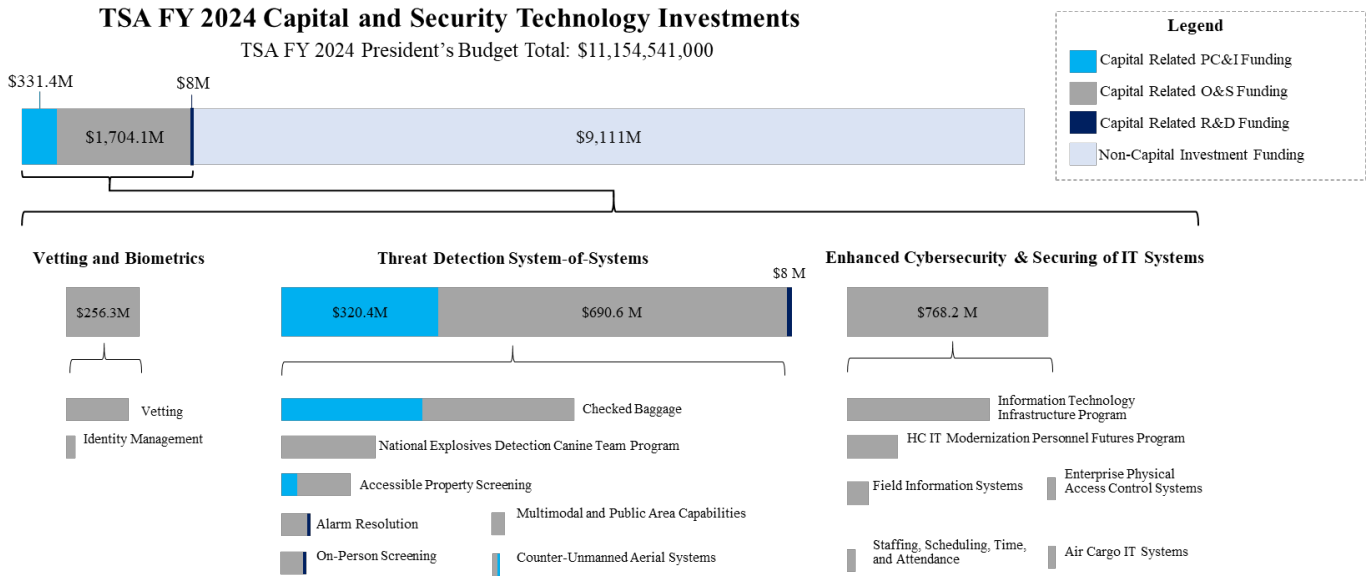
TSA by the Numbers

TSA is responsible for the security of passengers at more than 440 federalized airports within the aviation subsector. TSA daily screens more than 2 million passengers, 4.8 million carry-on items, and 1.1 million checked items for explosives and other dangerous items, preventing more than 6,500 firearms from entering airport secure areas in 2022. Travel volume returned to pre-pandemic levels last year, and in some locations, passenger volume has exceeded pre-pandemic volumes. TSA is prioritizing operational changes and rapid technology deployments that enable contactless and remote screening to support the rebound of domestic air travel and the post-Coronavirus Disease 2019 travel experience. As fewer passengers check bags, more space is available for air cargo. In addition, TSA provides aviation and air cargo regulatory compliance for the entire sector with 940 inspectors.

Across the surface subsector, TSA works closely with owners and operators to protect the critical physical and digital systems that connect cities, manufacturers, and retailers to power the economy through more than 4 million miles of roadways; nearly 140,000 miles of railroad track; more than 470 tunnels; and over 2.7 million miles of pipeline. TSA's security inspectors conduct approximately 8,000 surface inspections annually, using a risk-based approach.

Figure 1 shows the breakdown of capital-related investment in TSA's total budget.

Figure 1: TSA's Capital-Related Investment



Continuous and Sustained Investment

As the transportation security risk landscape evolves in response to new threats, demands, and technology advancements, TSA continues to invest in, acquire, and field new, sustainable solutions that strengthen the security of the transportation system, enhance the passenger experience, support movement of commerce, and advance the TSA workforce. Innovative security technologies, collaboration between stakeholders, a well-trained and dedicated security workforce, and a proactive approach to preparedness and resilience will all play a part in this evolution. The CIP, which covers the next 5 fiscal years' planned obligations, is based on the Future Years Homeland Security Program (FYHSP) authorized levels.[1] The CIP provides a cohesive overview of the capital investments required to: achieve TSA's strategic priorities; adapt to disruptions in the transportation ecosystem; and address complex future challenges within the FYHSP. **Figure 2** outlines TSA's FY 2024 budget request.

[1] 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 2024[2]

TSA Budget Request FY 2024 (Dollars in Thousands)												
	2022 Enacted			2023 Enacted			FY 2024 President's Budget Submission			2023 - 2024 Total Changes		
	Pos	FTE	$0	Pos	FTE	$0	Pos	FTE	$0	Pos	FTE	$0
Operations and Support	58,456	55,181	$8,091,193	61,932	56,193	$8,798,363	61,222	57,606	$10,331,752	-710	1,413	$1,533,389
Procurement, Construction, and Improvements	0	0	$160,736	0	0	$141,645	0	0	$81,357	0	0	-$60,288
Research and Development	0	0	$35,532	0	0	$33,532	0	0	$29,282	0	0	-$4,250
Appropriated Funds	**58,456**	**55,181**	**$8,287,461**	**61,932**	**56,193**	**$8,973,540**	**61,222**	**57,606**	**$10,442,391**	**-710**	**1,413**	**$1,468,851**
Vetting Fees - Discretionary	390	386	$458,650	390	386	$311,750	392	388	$456,150	2	2	$144,400
Mandatory Fees	19	19	$256,000	19	19	$256,000	19	19	$256,000	0	0	$0
Total Budget Authority	**58,865**	**55,586**	**$9,002,111**	**62,341**	**56,598**	**$9,541,290**	**61,633**	**58,013**	**$11,154,541**	**-708**	**1,415**	**$1,613,251**
Less Mandatory Fees	-19	-19	-$256,000	-19	-19	-$256,000	-19	-19	-$256,000	0	0	$0
Gross Discretionary	**58,846**	**55,567**	**$8,746,111**	**62,322**	**56,579**	**$9,285,290**	**61,614**	**57,994**	**$10,898,541**	**-708**	**1,415**	**$1,613,251**
Less Discretionary Vetting Fees	-390	-386	-$458,650	-390	-386	-$311,750	-392	-388	-$456,150	-$2	-$2	-$144,400
Appropriated Funds	**58,456**	**55,181**	**$8,287,461**	**61,932**	**56,193**	**$8,973,540**	**61,222**	**57,606**	**$10,442,391**	**-710**	**1,413**	**$1,468,851**
9/11 Passenger Security Fee Offset	0	0	-$2,368,503	0	0	-$2,490,000	0	0	-$4,204,000	0	0	-$1,714,000
Net Discretionary	**58,456**	**55,181**	**$5,918,958**	**61,932**	**56,193**	**$6,483,540**	**61,222**	**57,606**	**$6,238,391**	**-710**	**1,413**	**-245,149**

[2] FY 2024 Budget Request includes changes to the 9/11 passenger fee offset.

Strategic Alignment

The CIP represents the output of TSA's efforts to plan strategically and to enable continuous improvement in security, specifically with capital investments. The plan is built on the TSA Strategy, the Administrator's Intent, roadmaps (for example, Biometrics, Cybersecurity, Insider Threat, Air Cargo Security), Implementation Plans, and Strategic Priorities and Planning Guidance. The FY 2024 – FY 2028 CIP follows priorities set by TSA's FY 2024 – FY 2028 requirement prioritization process, which uses TSA risk and strategy documents in its quantified weighting and scoring approach. This approach considers how each priority addresses validated capability needs; enterprise, mission, and programmatic risks; and other enterprise strategies.

To achieve TSA's strategic vision, TSA aligns its capital investments with the following three pillars, displayed in **Figure 3**:

- Vetting and Biometrics
- Threat Detection System-of-Systems
- Enhanced and Secure IT Systems

Figure 3: CIP Summary Table FY 2024 – FY 2028

DRAFT CIP - FY 2024 - FY 2028 ($ in millions)						
Program	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 – FY 2028 Total**
A. Vetting and Biometrics						
I. Vetting	$227.5	$232.6	$235.8	$238.6	$241.2	**$1,175.7**
II. Identity Management	$28.8	$29.2	$29.1	$29.2	$29.2	**$145.5**
A. Vetting and Biometrics Subtotal	**$256.3**	**$261.8**	**$264.9**	**$267.8**	**$270.4**	**$1,321.2**
B. Threat Detection System-of-Systems						
I. Accessible Property Screening	$200.3	$200.6	$200.6	$200.6	$200.6	**$1,002.7**
II. Alarm Resolution	$53.7	$53.4	$53.4	$53.5	$53.4	**$267.4**
III. On-Person Screening	$47.8	$48.1	$48.1	$48.1	$48.2	**$240.3**
IV. Checked Baggage	$520.8	$521.3	$521.3	$521.3	$521.3	**$2,606.0**
V. Multimodal and Public Area Capabilities	$22.1	$22.1	$22.1	$22.3	$22.3	**$110.9**
VI. Counter-Unmanned Aerial Systems	$11.3	$11.5	$11.6	$11.7	$11.7	**$57.8**
VII. National Explosives Detection Canine Team Program	$163.0	$171.2	$178.6	$183.4	$186.9	**$883.1**
B. Threat Detection System-of-Systems Subtotal	**$1,019.0**	**$1,028.2**	**$1,035.7**	**$1,040.9**	**$1,044.4**	**$5,168.2**
C. Enhanced and Secure IT Systems						
I. IT Infrastructure Program	$391.9	$396.1	$396.9	$398.1	$399.0	**$1,982.0**
II. Cyber Security	$151.4	$135.4	$135.5	$135.7	$135.8	**$693.8**

DRAFT CIP - FY 2024 - FY 2028 ($ in millions)						
Program	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 – FY 2028 Total**
III. Field Information Systems	$38.1	$38.5	$38.5	$38.5	$38.5	**$192.1**
IV. Enterprise Physical Access Control System	$14.6	$14.6	$14.6	$14.7	$14.7	**$73.2**
V. Human Capital IT Modernization Personnel Futures Program	$142.5	$142.5	$142.5	$142.5	$142.5	**$712.5**
VI. Staffing, Scheduling, Time, and Attendance System	$16.4	$16.4	$16.4	$16.4	$16.4	**$82.0**
VII. Air Cargo IT Systems	$13.3	$13.3	$13.3	$13.3	$13.3	**$66.5**
C. Enhanced and Secure IT Systems Subtotal	**$768.2**	**$756.8**	**$757.7**	**$759.2**	**$760.2**	**$3,802.1**
Total	**$2,043.5**	**$2,046.8**	**$2,058.3**	**$2,068.0**	**$2,075.0**	**$10,291.5**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

The Need for Future Investment

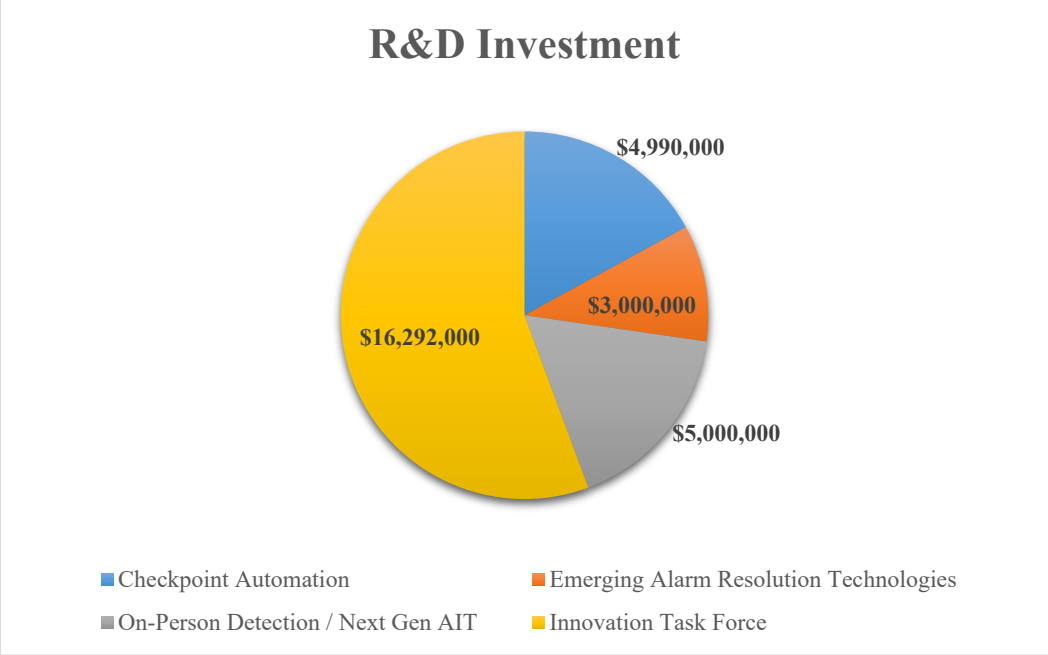
TSA requires screening technology to assist in deterring and detecting potential attacks. The ability to effectively execute its mission starts by arming its officers and workforce with the best technology capabilities available in time to mitigate known and emerging threats. TSA's existing systems are highly complex and proprietary, providing no standardized data, images, or interfaces. TSA will leverage existing contracts to continue investing responsibly in new equipment. However, a reliance on original equipment manufacturers (OEM) and existing contracting mechanisms for software, component, or operational upgrades limits TSA's flexibility and ability to engage with new and innovative partners to solve problems, increases development and acquisition costs, and impedes the response to emerging needs. The most critical advantage that TSA can retain over its adversaries is agility, including the ability to identify, test, and deploy solutions in response to threats.

Looking to the future, TSA requires productive and diverse partnerships and will seek to collaborate with industry, government, and academia stakeholders. These partnerships are essential to improving security effectiveness, ecosystem-wide innovation, operational efficiency, passenger experience, and workforce capabilities. TSA is committed to using all its authorities, partnerships, and capabilities to identify best-in-class solutions and to diversify the transportation security marketplace with emerging technologies. Two focus areas that highlight the importance of partnerships and market diversity in advancing TSA's capabilities are open architecture (OA) initiatives and research and development (R&D).

OA: TSA's introduction of open system software architecture elements into TSE is a pivotal investment in advancing TSA to a desired "system-of-systems" (SoS), risk-based screening future state. OA is a design approach where third-party components, such as software and hardware, are standards-based and interoperable to allow a wide range of industry partners to create improved subcomponents (for example, new detection algorithms, user interfaces, and reporting systems). TSA can leverage this approach to create a superior SoS that interact to provide a unique capability. Through OA, TSA provides pathways for new collaborators, enhancing innovation by broadening the market of possible partnerships and by allowing for greater flexibility to integrate best solutions that outmatch constantly changing threat environments. TSA expects OA will drive substantial increases in investment needs for both infrastructure and technology as activities further inform capability needs.

R&D: In addition to the Checkpoint Automation (CPAM) R&D work that supports OA, 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. TSA works with these organizations and private industry to ensure that efforts are not duplicative and that they support successful transition of technologies and solutions to the operational environment. The planned distribution of the FY 2024 R&D funds, totaling $29.3 million, is shown in **Figure 4**.

Figure 4: R&D Investment FY 2024



Capital Investment Plan
FY 2024–FY 2028

Table of Contents

I. Legislative Language 1

II. Plan Overview 4

III. Strategic Priorities to Drive Transformation 5
- A. Executing Our Mission 7
  - 1. Vetting and Biometrics 7
  - 2. Threat Detection System-of-Systems 9
  - 3. Enhanced Cybersecurity and Securing IT Systems 13
- B. Identifying and Prioritizing Threats, Risks, and Capability Needs and Gaps 14
  - 1. Enterprise Risk Management 14
  - 2. Transportation Sector Security Risk Assessment (TSSRA) 16
  - 3. Risk and Trade Space Portfolio Analysis (RTSPA) 16
  - 4. International Risk Framework (IRF) 16
  - 5. TSCAP 17
- C. TSA's Current State 18
- D. Defining an Ideal Future State 18
  - 1. OA 19
  - 2. CPAM Initiative 19
- E. Research and Development 20
- F. Partnering to Accelerate Action 21
  - 1. International Collaboration 21
  - 2. Expanding and Integrating Risk-Based Security 22
  - 3. Developing New and Improving Current Capabilities 22
  - 4. Support Threat Signature Characterization 22
  - 5. Passenger and Aviation Technology and Process Demonstrations 23
  - 6. Multimodal Transportation Technology 23
  - 7. Surface Security Technology (SST) 24

8. Capability Acceptance Process (CAP)....24
9. STSAC....24
10. Aviation Security Advisory Committee....25
G. Areas for Investment Opportunity (Unconstrained)....25

IV. Conclusion....28

Appendix....29

I. Capital Investment Programs (Constrained)....29
A. Vetting and Biometrics....29
1. Vetting....29
2. Identity Management....33
B. Threat Detection System-Of-Systems....39
1. APS....39
2. Alarm Resolution (AR)....44
3. On-Person Screening....48
4. Checked Baggage....52
5. Multimodal and Public Area Capabilities (MPAC)....56
6. Counter-Unmanned Aerial Systems (C-UAS)....64
7. National Explosives Detection Canine Team Program (NEDCTP)....66
C. Enhanced and Secure IT Systems....68
1. Information Technology Infrastructure Program (ITIP)....68
2. Field Information Systems (FIS)....72
3. Enterprise Physical Access Control System (ePACS)....75
4. Human Capital (HC) IT Modernization Personnel Futures Program....76
5. Staffing, Scheduling, Time, and Attendance System (SSTA)....77
6. Air Cargo IT Systems....78

II. PSP Legacy Program Funding Profile....79

III. Technology Acquisitions....80

IV. Compliance Matrix....83

V. Abbreviations....88

I. Legislative Language

This report addresses reporting requirements in the Joint Explanatory Statement accompanying the Fiscal Year (FY) 2023 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-328); 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 2023 DHS Appropriations Act (P.L. 117-328) includes the following requirements:

> Section 221. 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 Commerce, Science, and Transportation of the Senate and the Committees on Appropriations and Homeland Security in the House of Representatives 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 221. The agreement continues and modifies 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 mission of the Transportation Security Administration (TSA) is to protect the Nation's transportation systems and to ensure freedom of movement for people and commerce. For TSA to be well-equipped to execute its mission and to sustain and modernize operations, it must consider the overall transportation environment, current and future risks and threats, opportunities for partnership with industry, and policy and process innovation.

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

The FY 2024 – FY 2028 CIP summarizes the output of 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,"[3] 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.

Funding includes amounts for procurement, construction, and improvements (PC&I); operations and support (O&S); and research and development (R&D), as requested in the FY 2024 President's Budget and outyear requirements in the Future Years Homeland Security Program (FYHSP). An additional section, now required by legislation, highlights TSA's investments from an unconstrained perspective that also incorporates the current threat environment and capability forecast. The plan describes an ideal future state in which TSA can buy down more risk to the transportation sector, by maximizing investments in our PC&I funding.

[3] Executive Order 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 Transformation

TSA has four mutually reinforcing guidance documents that advance its strategic vision:

- The TSA Strategy,[4] which articulates the shared vision, goals, and priorities for TSA through 2027;
- Administrator's Intent,[5] which identifies near-term activities to advance the TSA strategy;
- The National Strategy for Transportation Security, a biennial plan that identifies and evaluates the Nation's transportation assets;[6] and
- The FY 2024 – FY 2028 Strategic Priorities and Planning Guidance, which is the culmination of the Planning phase within the Planning, Programming, Budgeting, and Execution – Strategy (PPBE-S) process and which guides resource allocation decisions in subsequent outyear programming, budgeting, and execution phases.

Throughout the FY 2024 – FY 2028 requirements prioritization process, TSA considered the TSA Strategy and the upcoming Administrator's Intent 3.0 with three key priorities: people, partnership, and technologies. Using a quantitative weighting and scoring approach, TSA considered how each requirement addresses validated capability needs; enterprise, mission, and programmatic risks; and other enterprise strategies. Priorities focus primarily on advancing aviation security and screening, progressing TSA's workforce and human capital systems, executing IT modernization, cybersecurity and protecting critical infrastructure, improving identity management (IDM) capabilities, and enhancing insider threat detection, deterrence, and mitigation. The CIP outlines capital investments that drive these priorities, advancing TSA's mission and strategic vision.

Transforming Mission Execution

The transportation ecosystem continues to evolve with new and dynamic threats and other unpredictable disruptions, including the lingering impacts of the Coronavirus Disease 2019 (COVID-19) pandemic and cybersecurity threats from state and non-state actors. Reflective of such, 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 passenger screening experience. To transform mission execution, TSA creates a security infrastructure comprised of capital investments and complementary policies, processes (for example, capability management), and strategic partnerships that collectively optimize security solutions, advance TSA's priorities, and strengthen transportation security.

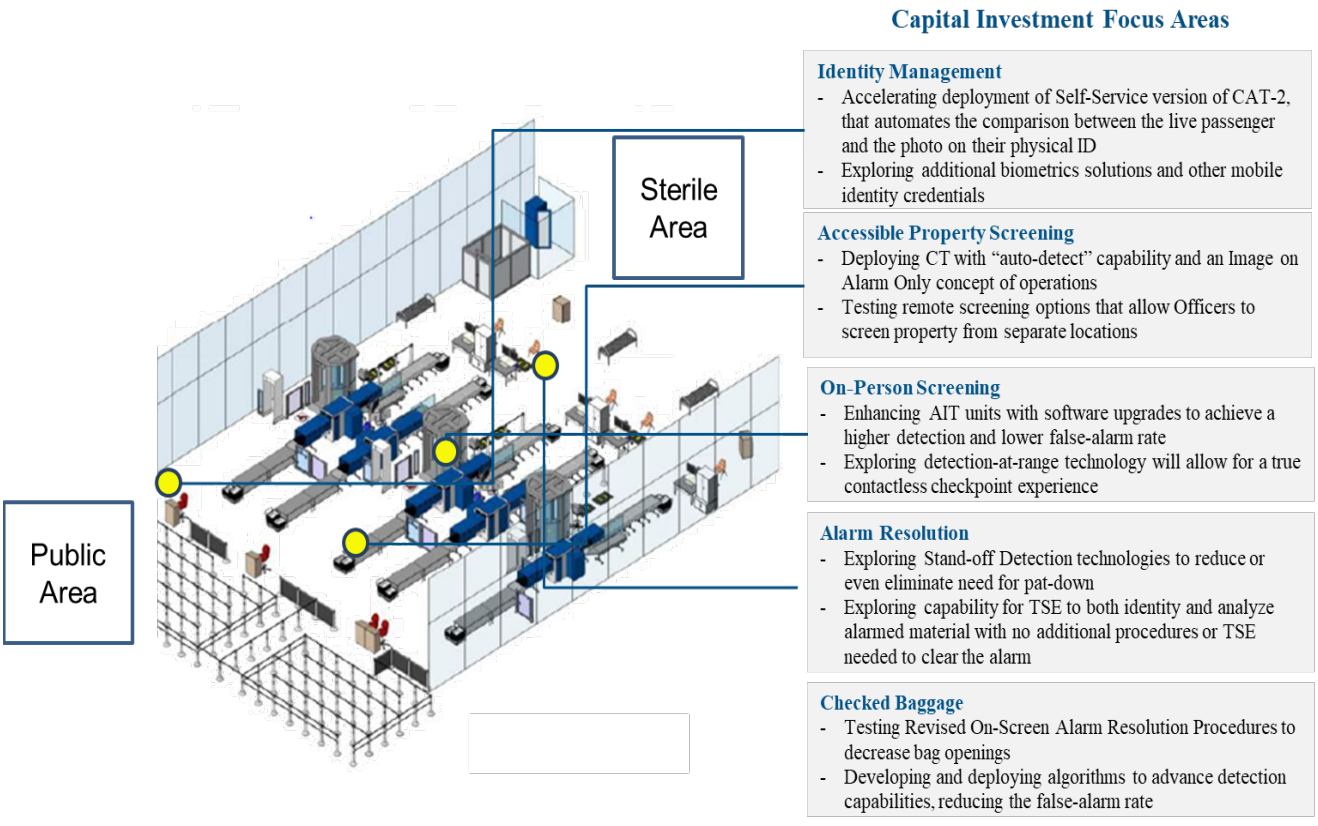
[4] TSA Strategy, 2018–2026: https://www.tsa.gov/sites/default/files/tsa_strategy.pdf
[5] Administrator's Intent 3.0 is currently under development
[6] 2020 Biennial National Strategy for Transportation Security: https://www.dhs.gov/publication/2020-biennial-national-strategy-transportation-security

While the COVID-19 pandemic heightened existing needs for TSA to evolve its approach to security screening, checkpoint design, and airport operations, an array of known and unknown threats will further drive those needs.

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

For example, TSA leveraged credential authentication technology (CAT), which validates passenger identity and vetting status, to develop Second Generation CAT (CAT-2), a self-service version of CAT with camera that has been deployed to certain locations. Similarly, TSA is looking to improve its screening of accessible property through the deployment of checkpoint computed tomography (CT) with "auto-detect" capability and an 'Image on Alarm Only' concept of operations. TSA is also working to integrate advanced detection algorithms into the On-Person Screening (OPS) equipment capabilities. **Figure 5** depicts how these investments and others within the airport environment are creating the checkpoint of the future.

Figure 5: Capital Investment/Capability Focus Areas within the Airport Environment



The investments needed to execute and transform the mission are spread across the following mission areas: 1) Vetting and Biometrics, 2) Threat Detection System-of-Systems (SoS), and 3) Enhanced and Secure IT Systems. To advance these pillars, TSA invests in R&D; engages with partners across government, industry, and the traveling public; and identifies policy and process improvements to optimize investments.

To realize the full potential of checkpoint technologies, TSA also is investing in:

- Key Open Architecture elements to support rapid deployment of capability to the field.
- IT systems including the Security Technology Integration Program (STIP), which pushes system-wide detection software updates more rapidly than current manual processes that are implemented machine-by-machine.
- Modernization of mission support systems to manage changes in staffing operations of its almost 50,000 TSOs to allow for more automation and agility.
- Facility maintenance and real estate.

Continued transition to a capability management operating model is an important process shift that enables TSA both to transform transportation security and to identify the investments needed to do so. This operating model designates a single capability manager (CM) to build the future state roadmap for a capability, to improve integration, and to take a more comprehensive approach to security solutions. CMs further integrate technologies into the field by considering nonmaterial aspects of solutions (procedures, training, etc.), driving seamless connections of their capability to other TSE identifying solutions that reduce contact in screening, improving the passenger experience, and advancing TSA toward a mature screening SoS. Current CMs support TSA's fielded capabilities and include most of TSA's capital investment programs.

A. Executing Our Mission

1. Vetting and Biometrics

At TSA, vetting is the process of determining whether individuals seeking access to the transportation environment are potential threats by screening them according to their risk status. Vetting is a critical part of IDM and works in tandem with identity proofing and identity verification to ensure that TSA enables the right persons to be granted the right access or credential based on their biographic and biometric information.

Prior to arrival at a checkpoint, the Secure Flight program enhances security by identifying low- and high-risk passengers before they arrive at the airport by matching names against trusted traveler lists and watchlists. This process also minimizes misidentification of individuals. Currently, Secure Flight operates with CAT, through the connection with STIP, to identify occurrences in which the name screened by Secure Flight does not match the boarding pass and/or passenger identity or travel document presented. It also verifies a passenger's vetting status against the Secure Flight database in near real-time (NRT) so that the passenger receives the appropriate screening based on TSA's assessed risk. This maturation of the system and operations will include a built-in, two-way communication capability between Secure Flight and

CAT, enabling NRT assessments that will drive operational planning and responses and will provide feedback to the intelligence community.

In addition to maturing the Secure Flight program, TSA continues to enhance its use of biometrics. TSA published its Biometrics Roadmap[7] in 2018 and its Identity Management Roadmap[8] in 2022 to detail the agency's plan to evolve IDM into a more formalized and integrated capability across the enterprise. For example, TSA has developed and deployed the self-service version of CAT with the CAT-2 solution that builds on the existing CAT infrastructure, leverages the biometrically enabled prototype, and includes a self-service passenger-facing user interface. Camera functionality increases security effectiveness by automating the comparison between the live passenger and the photo on their physical identification document (ID). Automation eliminates vulnerabilities associated with social engineering and cognitive fatigue and thereby allows officers to focus their training and contextual judgment on anomalies rather than on visual facial comparisons. Additional funds are required to fully execute this upgraded solution nationwide, which is highlighted further in the IDM capability annex.

TSA is developing a facial identification solution of CAT-2 using a back-end repository to compare a live-image capture of consenting eligible travelers to a gallery of enrolled facial reference images and is exploring the use of digital identity capabilities. In addition, with the increased need to shift to contactless and automated screening, CAT-2 is designed to automate existing high-touch actions.

TSA is working closely with its vendor base, commercial aviation stakeholders, and interagency partners at DHS, including U.S. Customs and Border Protection (CBP) and the Office of Biometric Identity Management to ensure that TSA's identity solutions minimize technical bias and are standards-based, user-friendly, and scalable, and to address TSA mission needs while protecting passengers' privacy and civil rights and liberties. Fostering communication, transparency, and input regarding the development of biometric solutions from stakeholders remains a key part of TSA's overall strategy.

TSA continues to mature its risk-based approach to increase the use of biometrics screening, to improve confidence in security verification, and to minimize the risk of adversary manipulation through priority investments in the IDM portfolio focused on: digital identity technology, and identity proofing and enrollment. Implementation of IDM capabilities requires systems integration, biometric system improvements, data analytics and algorithm development, cybersecurity, and standardization and requirements. These IDM capabilities will ensure a safe and secure TSA checkpoint as technology continues advancing and as adversaries find new methods of attack.

Figure 6 shows the funding aligned to vetting and biometrics projects and programs from the FY 2024 Congressional Justification (CJ) and TSA's FY 2024 – FY 2028 FYHSP. Security-related

[7] TSA Biometrics Roadmap (2018): https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf

[8] TSA Identity Management Roadmap (2022): https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf

technology (SRT)[9] programs are noted for traceability requirements in the 5-year technology investment plan requirements.

Figure 6: Vetting and Biometrics FY 2024 – FY 2028

A: Vetting and Biometrics – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Vetting & Credentialing System	$88.6	$88.6	$88.6	$88.6	$88.6	$443.0
Secure Flight	$138.9	$144.0	$147.2	$150.0	$152.6	$732.7
Total Vetting	**$227.5**	**$232.6**	**$235.8**	**$238.6**	**$241.2**	**$1,175.7**
Credential Authentication Technology	$14.6	$16.4	$17.2	$18.9	$20.0	$87.1
Identity Investment	$2.3	$2.6	$2.6	$2.6	$2.6	$12.7
Boarding Pass Scanner	$0.9	$0.9	$0.9	$0.9	$0.9	$4.5
Subtotal O&S	**$17.8**	**$19.9**	**$20.7**	**$22.4**	**$23.5**	**$104.3**
CAT	$11.0	$9.3	$8.4	$6.8	$5.7	$41.2
Subtotal PC&I	**$11.0**	**$9.3**	**$8.4**	**$6.8**	**$5.7**	**$41.2**
Total Identity Management	**$28.8**	**$29.2**	**$29.1**	**$29.2**	**$29.2**	**$145.5**
Total Vetting and Biometrics	**$256.3**	**$261.8**	**$264.9**	**$267.8**	**$270.4**	**$1,321.2**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

2. Threat Detection System-of-Systems

The checked baggage and checkpoint systems address emerging and evolving terrorist threats to commercial aviation security. TSA must invest in new technologies and processes as well as in automation, integration, and connection. These investments will create a mature aviation screening system-of-systems that strengthens TSA's security posture, creates efficiencies, improves the passenger experience, protects the workforce, and responds dynamically to threats and disruptions.

TSA continues to mature the accessible property screening (APS) capability by deploying checkpoint CT systems with sophisticated algorithms. These systems offer an enhanced imaging platform with three-dimensional images compared to legacy two-dimensional Advanced Technology X-rays and they can detect a broader range of threats. TSA implemented the Checkpoint Property Security System (CPSS) Acquisition Program in 2019 to deploy a long-term CT solution incrementally with enhanced threat detection algorithms, ingress/egress, and networking capabilities.

[9] SRT is defined as any technology or related engineering services to deployed technology that assists TSA in the prevention of, or defense against, threats to U.S. transportation systems, including threats to people, property, and information. Engineering services are defined further as services that would result in new capabilities, enhancements of existing capabilities, or otherwise would upgrade an existing operational SRT. This definition does not include SRT that is procured for the purpose of demonstrations, prototype SRT, or SRT used for R&D purposes.

TSA's mid-term goal is to continue working toward employment of an "auto-detect" capability for explosive threats and non-explosives prohibited items, such as firearms, firearm components, and knives. TSA intends to introduce an 'Image on Alarm Only'[10] concept of operations that ultimately will improve checkpoint efficiency, will reduce staffing requirements, and will decrease the number of bags that require review/secondary screening, thus limiting the touch rate between TSOs and passengers' property. In addition, TSA aims to introduce OA concepts to CPSS systems through the adoption of the Digital Imaging and Communications in Security (DICOS) common image format and Open Platform Software Library (OPSL) standardized interfaces. As part of this work, DICOS provides standard image formatting across vendor solutions, while Threat Recognition System (TRS) allows for that integration of third-part algorithms. Introduction of these concepts will enable more advanced functionality in the long-term, regardless of vendor. This functionality will include the ability to support multiple algorithms to improve detection performance, standardization of operator interfaces through the Common Workstation, and implementation of risk-based screening concepts.

In addition, TSA is focused on enhancing Advanced Imaging Technology (AIT), the OPS capability technology that uses millimeter waves to detect concealed items on passengers. These enhancements will improve the passenger experience and advance security by achieving increased throughput and enhanced detection standards, eliminating most checkpoint bottlenecks associated with passenger screening. As a result, TSA's move to contactless screening will be accelerated as the need for physical pat-downs decreases. TSA is updating AIT units with advanced algorithms, including low probability of false alarm[11] algorithms that are gender-neutral, reducing secondary screening and enhancing security effectiveness. This is in line with the President's EO 13988, "Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation."[12]

To reduce false-alarm rates further, TSA is continuing to invest in its secondary screening technologies, including Alarm Resolution (AR) and Advanced Alarm Resolution (AAR) operations. In advancing these screening methods to the next-generation capability, TSA will focus on alarmed items in containers or concealments that do not allow access for sampling, a contactless capability for AR, and implementation of automation and reduction of labor-intensive processes, which will reduce secondary screening and time it would otherwise take to transit through the checkpoint. Regarding checked baggage, TSA continues to work toward its goal of detecting more threat materials at lower threat mass, lower false-alarm rates, and lower lifecycle costs.

[10] Addressing the threat posed by improvised explosive threats, DHS S&T awarded a contract to develop and implement an automatic threat resolution system for use with X-ray imaging of carry-on and checked baggage. It will integrate an advanced X-ray diffraction system with automatic threat resolution capabilities into an existing dual-view, advanced-technology screening system currently used at airport checkpoints.

[11] The fraction of all items not containing a true threat for which the system incorrectly declared an alarm. To be used as a metric.

[12] Executive Order on Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-preventing-and-combating-discrimination-on-basis-of-gender-identity-or-sexual-orientation/

Within the OPS capability, TSA continues exploring detection-at-range capabilities that focus on screening at speed and at distance, which reduces contact and enhances the passenger experience. As CBP has used detection-at-range capabilities, TSA is interested in this non-intrusive technology that specifies effective distance for recognizing a target, object, or other type of threat. TSA will invest in new technology that can increase passenger throughput, enhance detection standards, and connect to a secure network. TSA also will invest in R&D for next-generation OPS technologies that can screen passengers automatically at speed, detect reduced threat masses, discriminate between different materials, and promote a more contactless checkpoint.

TSA maintains responsibility for investing in technologies and other solutions to protect the multimodal and public areas from persistent threats. TSA leverages its robust abilities in capability gap identification, scouting, testing, evaluation, and deployment assistance to integrate security technologies into airport infrastructure, surface transportation, air cargo, and public area test beds. Partnering with representative and higher threat venues through formal memoranda of agreement allows TSA to establish roles and responsibilities for the planning, installation, operation, and maintenance of TSA-sponsored air cargo and surface test beds. TSA's test beds provide a critical capability for evaluating the operational performance and suitability of new technologies in surface transportation environments. Technologies tested through TSA's test bed process provide multiple data sets and feedback from a wide variety of users to inform evaluation analysis. The evaluations offer system partners extended access to and use of promising technologies before any procurement decisions.

Within this space, TSA also focuses on combatting growing unmanned aerial system (UAS) threats by investing in multiple test beds to assess technologies for counter-UAS (C-UAS), most recently at Miami International (MIA) and Los Angeles International (LAX) airports. No marketplace systems have been tested comprehensively in a complex civilian, metropolitan airport environment. Many airport authorities are acquiring UAS detection, tracking, and identification systems independently because of recent negative impacts of UAS to commercial aviation and the lack of federal capabilities. The lack of centralized federal guidance, however, poses risks at airports and results in operational and procurement inefficiencies with the deployment of disparate systems. The White House and Congress have made significant efforts to authorize state, local, tribal, and territorial (SLTT) entities to conduct C-UAS operations. TSA expects these efforts to gain momentum in upcoming years.

Figure 7 shows the funding aligned to enhanced threat detection projects and programs from the FY 2024 President's Budget and TSA's FY 2024 – FY 2028 FYHSP.

Figure 7: Threat Detection System-of-Systems FY 2024 – FY 2028

B: Threat Detection System-Of-Systems – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Accessible Property Screening	$129.9	$130.2	$130.2	$130.2	$130.2	$650.7
Alarm Resolution	$50.7	$50.4	$50.4	$50.5	$50.4	$252.4
On-Person Screening	$42.8	$43.1	$43.1	$43.1	$43.2	$215.3
Checked Baggage	$270.8	$271.3	$271.3	$271.3	$271.3	$1,356.0
Multimodal and Public Area Capabilities	$22.1	$22.1	$22.1	$22.3	$22.3	$110.9
C-UAS	$11.3	$11.5	$11.6	$11.7	$11.7	$57.8
National Explosives Detection Canine Team Program	$163.0	$171.2	$178.6	$183.4	$186.9	$883.1
Subtotal O&S	**$690.6**	**$699.8**	**$707.3**	**$712.5**	**$716.0**	**$3,526.2**
Checkpoint Property Screening System PC&I	$70.4	$70.4	$70.4	$70.4	$70.4	$352.0
ASCF (Aviation Screening Capital Fund) - Electronic Baggage Screening Program - Investment	$250.0	$250.0	$250.0	$250.0	$250.0	$1,250.0
Subtotal PC&I	**$320.4**	**$320.4**	**$320.4**	**$320.4**	**$320.4**	**$1,602.0**
Emerging Alarm Resolution Technologies	$3.0	$3.0	$3.0	$3.0	$3.0	$15.0
On-Person Detection/Next Gen Advanced Imaging Technology	$5.0	$5.0	$5.0	$5.0	$5.0	$25.0
Subtotal R&D	**$8.0**	**$8.0**	**$8.0**	**$8.0**	**$8.0**	**$40.0**
Total Threat Detection System-Of-Systems	**$1,019.0**	**$1,028.2**	**$1,035.7**	**$1,040.9**	**$1,044.4**	**$5,168.2**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

3. Enhanced Cybersecurity and Securing IT Systems

The President's EO 14028, "Improving the Nation's Cybersecurity"[13] in conjunction with the Office of Management and Budget's (OMB) strategy to move the U.S. Government toward zero trust architecture, requires TSA to migrate to a "zero trust" framework and to ensure that baseline security practices are in place. TSA realizes the security benefits of migrating to a cloud-based infrastructure while mitigating associated risks.

To migrate to a defensible zero trust architecture and to enhance cybersecurity resilience of the Transportation Systems Sector, TSA continues to protect the confidentiality, integrity, and availability of its systems, data, and information by: staying ahead of cybersecurity threats and vulnerabilities, modernizing IT systems, and increasing connectivity between TSE.

As one of the co-Sector Risk Management Agencies for the Transportation Sector Security (TSS), TSA partners with federal, state, and local stakeholders, as well as critical infrastructure owners and operators to reduce the risk of unauthorized access to information systems and equipment. One way this is done is to identify and conduct research to provide access to technology for owners and operators enabling them to buy down risk. This includes a technology platform TSS owners and operators can use to identify potential gaps in their existing cybersecurity policies and procedures against different cyber threat attack vectors.

TSA's current system has limited capabilities for rapidly transferring and standardizing information in support of operational decision-making. The limited capabilities are derived from TSA's use of legacy screening equipment, which fails to address cybersecurity requirements adequately as outlined in DHS 4300-A and the Federal Information Security Management Act (FISMA). TSA has imposed mitigation strategies to offset the associated risks, which have caused the limited capabilities of screening systems and technology. Capital investment in the IT Infrastructure Program (ITIP) and other TSA technology programs, will provide modern IT services, including those related to securing and enhancing TSA's ability to collect, process, and analyze data, and to transfer voice, video, or digital information. Checkpoint Automation (CPAM), currently in the R&D phase, will focus on edge computing to move data at the checkpoint in real-time while the mature STIP capability has connected TSE to a single network and enables enhanced cybersecurity effectiveness, information sharing, and data management and backend data collection analyses.

In addition to screening equipment, TSA incorporates mandatory IT standards for monitoring, protecting, and addressing cybersecurity threats and vulnerabilities in its IT systems such as the Vetting and Credentialing System and Secure Flight, for example. The majority of these systems' cybersecurity investments are focused on hardware and software security. TSA is also assessing internal opportunities to evaluate, procure, and implement cutting-edge tools, capabilities, and analytical products that could help target opportunities for improving cybersecurity resiliency and preparedness across the transportation sector. To optimize operational efficiency, TSA seeks to invest in modernizing existing mission support functions.

[13] Executive Order 14028 on Improving the Nation's Cybersecurity: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The COVID-19 pandemic accelerated the need to modernize IT support functions. Modernizing human capital and scheduling infrastructure, like the Federal Air Marshal Service's Mission Scheduling and Notification System (MSNS) and the Staffing, Scheduling, Time, and Attendance (SSTA) system would allow TSA to adapt and respond better to major disruptions and to automate critical day-to-day operations.

As TSA looks to the future, it will continue to focus on the transparent management of IT modernization, cloud computing, real-time data analytics, artificial intelligence, and cybersecurity.

Figure 8 shows the funding aligned to IT Systems Enhancement projects and programs from the FY 2024 President's Budget and TSA's FY 2024 – FY 2028 FYHSP.

Figure 8: Enhanced and Secure IT Systems FY 2024 – FY 2028

C. Enhanced and Secure IT Systems – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 – FY 2028 Total**
IT Infrastructure Program (ITIP)	$391.9	$396.1	$396.9	$398.1	$399.0	$1,982.0
Cyber Security[14]	$151.4	$135.4	$135.5	$135.7	$135.8	$693.8
Field Information Systems (FIS)	$38.1	$38.5	$38.5	$38.5	$38.5	$192.1
Enterprise Physical Access Control System (ePACS)	$14.6	$14.6	$14.6	$14.7	$14.7	$73.2
Human Capital (HC) IT Modernization Personnel Futures Program (PFP)	$142.5	$142.5	$142.5	$142.5	$142.5	$712.5
Staffing, Scheduling, Time, and Attendance (SSTA) System	$16.4	$16.4	$16.4	$16.4	$16.4	$82.0
Air Cargo IT Systems	$13.3	$13.3	$13.3	$13.3	$13.3	$66.5
Total Enhanced and Secure IT Systems	**$768.2**	**$756.8**	**$757.7**	**$759.2**	**$760.2**	**$3,802.1**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

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

TSA needs sufficient funding to continue to evolve 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 is a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision-making for

[14] $118 million of the Cyber Security investment is also included within ITIP internal cybersecurity funding.

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, reflected in **Figure 9,** 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.

Figure 9: TSA Enterprise Risk Register

Risk	Risk Statement
Screening Capacity	IF TSA fails to adapt screening operations (equipment deployments, functionality as intended, and screening procedures) to account for passenger volume trends, THEN it increases the chance of security vulnerabilities (lanes down, lanes underperforming, lanes equipped with inadequate functionality)
Insider Threats	IF complexities in mitigating, detecting, and responding to an insider threat persists, THEN it increases the likelihood of an attack perpetrated or enabled by transportation insiders.
Screening Capability	IF TSA lacks resources to strengthen critical capability areas (such as Identity Management, On-Person Screening, Accessible Property Screening, Checked Baggage, and Alarm Resolution) to identify gaps, needs, and requirements and implement solutions, THEN it increases the ability of an adversary to carry out an attack on the aviation transportation system.
Workforce Retention	IF TSA is unable to acquire, develop, and retain talent across the Agency due to insufficient resources to develop leaders; ensure diversity, equity, inclusion, and accessibility; and provide equitable compensation, THEN it impedes execution of the mission and undermines morale.
Surface Transportation	IF TSA is unable to obtain, analyze, and share information with stakeholders about potential cascading impacts and improve compliance rates to the surface transportation sector (e.g., digital and physical), THEN its ability to improve resiliency across the sector would be compromised.
Enterprise Data Management	IF TSA fails to make data findable, accessible, interoperable, and reusable throughout the agency, THEN it results in decisions based on insufficient information.
TSA Cybersecurity (Internal)	IF TSA fails to prevent or address cyberattacks and associated information technology breaches in TSA-managed and/or third-party vendor networks and equipment, THEN it leads to unauthorized access to information, degraded services/operations (e.g., screening, vetting, credentialing, Secure Flight, Law Enforcement/Federal Air Marshal Service (LE/FAMS)), and/or commerce and travel disruptions.

Transportation Systems Sector (TSS) Cybersecurity	IF TSA fails to mitigate cyberattacks/breaches to information systems and equipment within the TSS (e.g., pipelines, passenger rail, public transportation, freight rail, aviation, air cargo), THEN it enables unauthorized access to information or severe disruptions to commerce and travel that can adversely affect other critical infrastructure sectors.
Enterprise Performance Metrics	IF TSA does not establish a framework for applying and analyzing enterprise performance metrics, THEN it impedes the agency's ability to evaluate the impact of critical policies.
Emerging and Evolving Threats	IF TSA fails to effectively leverage technology, human capital, process, and policy solutions for intelligence efforts, THEN it will not be able to forecast and mitigate new threats.
Modernizing Enterprise Support Technology	IF TSA lacks modernized enterprise support technology, including material and non-material solutions, THEN it reduces the agency's ability to fulfill mission essential functions.
Decision-Making Processes	IF TSA fails to execute, maintain and manage efficiently documented governance processes and practices, THEN the agency cannot fully implement the Administrator's Intent and other strategic priorities.

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. TSSRA's scenarios and overarching risk landscape support TSA decision-makers across a variety of resourcing, security, and policy considerations, and contribute to the Transportation Security Capability Analysis Process (TSCAP) described below.

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 TSCAP, and the PPBE-S processes.

4. International Risk Framework (IRF)

The IRF evaluates the relative risk of a terrorist attack onboard an international flight inbound to the United States from a last-point-of-departure (LPD) airport. The IRF evaluates the risk components of 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. 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 CMs 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 pillars and the capital investment/capability focus areas:

- **Vetting and Biometrics**
  - *IDM and Vetting*: Ensuring the effective and efficient integration of identity-related activities and prioritization of resources including enrollment, validation, vetting, authentication, and verification processes throughout the enterprise.
- **Threat Detection System-of-Systems**
  - *Accessible Property:* Enhancing the security effectiveness and operational efficiency of TSA's APS through automation, integration, and connection.
  - *AR:* Advancing material and nonmaterial capabilities to identify, analyze, and resolve alarms accurately within the TSA security ecosystem.
  - *OPS:* Improving TSA's OPS capabilities, including AIT, walk-through metal detectors, pat-down procedures, and other emerging capabilities.
  - *Checked Baggage:* Advancing effective and efficient material and nonmaterial solutions in the checked baggage space.
  - *Multimodal:* Providing security technology recommendations and solutions for air cargo, public transportation areas, and critical infrastructure (for example, pipelines) by evaluating existing security technologies, by developing requirements for new technologies, by partnering with national labs and cybersecurity researchers and vendors to develop assessment tools, and by stimulating the technology marketplace.
  - *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.

- **Enhanced and Secure IT Systems**
  - *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.

C. TSA's Current State

To date, TSA has addressed ever-present threats to aviation, but also anticipated dynamic and emerging cybersecurity threats to our Nation's aviation, rail, and oil and gas pipeline infrastructure, as well as evolving public health threats, such as COVID-19. 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.

Because the threat landscape is constantly evolving and passenger volumes have returned to pre-pandemic levels, TSA must continue to invest in, acquire, and field new technologies to strengthen transportation security, deal with evolving threats, and remain flexible with the evolving nature of the transportation system.

D. Defining an Ideal Future State

The transportation system is continuing to evolve with adversaries changing the threat landscape and increasing capacity demands. To meet its mission, TSA continues to advance security solutions to deter or defeat attacks and to adapt to disruptions in the transportation security ecosystem.

Along with policy, process, and partnership enhancements that optimize its capital investments, TSA prioritizes emerging and interconnected technologies and will continue developing solutions that seamlessly connect the cyber-physical space in an OA environment. Technologies enabling these capability improvements include biometrics, machine learning, cloud computing, and use of a variety of new sensors or improvements to existing systems. Investments in these areas and achieving economies of scale by connecting TSE to more efficient centralized security functions will allow for long-term improvements in TSA's overall performance.

CM, in collaboration with program managers and other stakeholders, will continue to provide enterprise oversight for TSA capability areas throughout their lifecycle. This oversight will help ensure proper resourcing and alignment to DHS and TSA strategies and priorities. TSA must

continue to fund deficiencies in specific capability management areas to stay ahead of the rapidly changing threat landscape within aviation and surface modes of transportation.

1. OA

TSA's current systems are complex and proprietary with little data, image, or interface standardization. TSA therefore relies on the original equipment manufacturers (OEM) and existing contracting mechanisms for software, algorithm, component, or operational upgrades. This limits TSA's ability to engage with new and innovative partners, increases development and acquisition costs, and can impede the response to emerging needs. TSA has begun establishing an OA environment through the CPAM initiative to address current systems challenges, reduce time to field solutions, diversify the marketplace, and promote international security screening objectives, as demonstrated in the recently published OA for Airport Security Systems document and the OA Roadmap[15]. From an industry perspective, OA enables vendors to compete for multiple awards and acquisitions targeted to specific components which reduce the risks and up-front investment associated with delivering a complete solution for a single award. In addition, vendors can more easily participate within different segments of the market depending on their business model. TSA currently operates much of its research and development, as well as capability procurement activities in a vendor-locked space that poses its own challenges, including:

- Long system/solutions development and evaluation lead times;
- Proprietary system designs and limited understanding of security requirements;
- Competition and innovation barriers presented by potentially limited resources and unconducive procurement strategies; and
- Limited ability to share threat, passenger, and risk information.

2. CPAM Initiative

The CPAM initiative will provide the TSA programs with the information and requirements necessary to enable the incremental implementation of open architecture solutions to: advance risk-based screening objectives, enable modularity, reduce costs, enhance innovation through a diversified market, and expedite the delivery of capabilities.

TSA's introduction of open system architecture elements into TSE through the CPAM initiative's developmental and demonstration activities is a pivotal priority in advancing TSA toward the future state. OA provides more pathways for new collaborators, enhances innovation through broadening the market of possible partnerships, and allows for greater options to identify the best solutions to outmatch the constantly changing threat environment. The following components of CPAM support TSA's achievement of its open architecture vision of the future:

[15] Open Architecture for Airport Security Systems: https://www.aci-europe.org/downloads/resources/Open%20Architecture%20for%20Airport%20Security%20Systems_1st%20Edition.pdf.

- DICOS Adoption: Continued development of the standardized data format (DICOS v3.0) and associated toolkits for capturing scanner data and providing in a nonproprietary format;
- OPSL Development: Standardizes data exchanges within systems to allow for integration of new equipment;
- Stream-of-Commerce Data Collection: Collects and documents stream-of-commerce images and associated meta-data in an efficient manner;
- Passenger Baggage Object Database Establishment: Stores and catalogs threat and stream-of-commerce data to support sharing with industry partners and government test facilities;
- Common Workstation Development: Standardizes the physical and graphical user interfaces across baggage scanners; and
- Threat Recognition System Development: A server connected to OEM systems that leverages OPSL and DICOS to allow for the use of a suite of algorithms from OEMs, third parties, and academia.

3. Real Estate

TSA's Real Estate program must focus limited resources on paying rent, utilities, and operating expenses and addressing only the most critical repairs and maintenance activities for TSA's leased and owned real property portfolio. Annual Real Estate shortfalls inhibit TSA's ability to provide a safe and secure working environment with appropriate facility conditions and furnishings for the TSA front line workforce. To ensure the program is operating at optimal capacity, future investment is required for TSA to keep pace with significant cost escalations in rent and operating costs, proactively address critical building lifecycle repairs/maintenance, and address the backlog of more than $30 million in deferred projects required to bring TSA field locations to an appropriate condition for front line employees

E. Research and Development

TSA depends on sustained and coordinated investment in research, development, testing, and evaluation to achieve its vision for the future state and to respond to known or emerging threats with timely solutions. 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. Alongside these partners, TSA coordinates relevant R&D activities across organizations to eliminate duplication and to maximize the adoption of applicable technologies. As an operational Component, TSA focuses its R&D funds on capability developments through enhancements across people, processes, and technology with the greatest mission impact.

TSA works with DHS S&T to shape capability development throughout the acquisition process by identifying capability gaps, by defining requirements, and through testing and evaluation, as well as through systems engineering expertise and operational analysis. Collaboration with S&T

encompasses R&D at many stages from basic research to technology development, scouting, and demonstration, and includes topics as varied as homemade explosive characterization to advanced detection algorithm development.

TSA facilitates R&D activities and infrastructure protection across the Nation's other transportation modes (mass transit and passenger rail, freight rail, pipeline, maritime terminals, transportation public areas) by evaluating and communicating a technology's effectiveness. This approach helps to stimulate the marketplace, to spark innovation, and to streamline end-user access to advanced and proven capabilities.

TSA's R&D priorities for the next five years align to the following focus areas:

- Enhanced threat detection for aviation and multimodal screening systems: Investing in operationally feasible primary and secondary screening systems with higher levels of detection across a broader range of threat types;
- Improved systems and processes for screening performance, passenger experience, and officer safety: Driving forward advances in emerging technologies and applying them to transportation security use cases to foster a safer, more seamless traveling experience; creating a more connected, interoperable, and open systems architecture; and unlocking cost efficiencies and greater detection performance; and
- Expansion of R&D partnerships across the public and private sectors: Fostering a broader network of close partners across the public and private sectors who are committed to helping TSA advance domestic and global security standards.

F. Partnering to Accelerate Action

TSA requires productive and diverse partnerships to achieve its mission and constantly seeks to collaborate more effectively with industry, government, and academic stakeholders. Examples of these initiatives are detailed below:

1. 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 through direct relationships with specific states or member groups. Open dialogue helps to build and enforce joint standards, to align R&D efforts, and to test emerging capabilities to improve the global security landscape. TSA has worked with the Airports Council International-Europe for OA collaboration. Airports Council International-Europe published the "Open Architecture for Airport Security Systems" paper in 2019 and is in the process of updating and developing additional products with the goal of defining common standards and interfaces across vendors, regulators, and airports. In addition, TSA has collaborated with, and now leads, the Aviation Cybersecurity Initiative. Through the Aviation Cybersecurity Initiative, TSA will engage with vendors, airport owners and operators, international partners, and its U.S. Government partners on technology updates with a goal of defining common standards and interfaces.

2. Expanding and Integrating Risk-Based Security

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. As PreCheck® makes up roughly 25 percent of the traveling public, every additional enrollee is 1 less passenger that would otherwise be subject to full standard screening process.

3. Developing New and Improving Current Capabilities

TSA collaborates with academia, industry, interagency, and international partners to identify and integrate technology and to process advancements into existing security systems to enhance security effectiveness and to improve operational efficiency. Working with vendors, airports, and airlines, TSA continues identifying emerging technologies that improve security, the passenger experience, and efficiency, and piloting them in live field environments. Initiatives such as the secure mobile application(s) associated with the Checkpoint Information Management (CIM) pilot will coordinate the handling of data gathered during operational reporting of incidents at airport checkpoints. Some concepts that the pilot aims to evaluate and improve upon include delivering more real-time incident reporting, providing for increased LE/FAMS need for information-sharing systems, and assessing application deployment, training, and support. These modernization initiatives and the CIM pilot will benefit TSA's stakeholders, mission sets, and strategic priorities by: modernizing legacy applications, standardizing data, minimizing duplicate data entry, addressing cybersecurity issues, reducing system maintenance costs, and promoting better integration with other applications as they are introduced. TSA seeks to further its collaboration with the Federal Railroad Administration to advance shared objectives for the expansion and use of the Transportation Technology Center in Pueblo, Colorado. This joint effort will further enhance the capability of this facility to support government and commercial entities in achieving the broader mission of transportation safety, reliability, efficiency, automation, connectivity, security, and overall innovation.

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 TSEs. These new algorithms use machine-learning approaches to discriminate between threats and benign objects, making the screening process more effective and efficient.

5. Passenger and Aviation Technology and Process Demonstrations

TSA's Innovation Task Force (ITF) is a collaboration among TSA, manufacturers, and airports to demonstrate emerging technological, automated, ergonomic, environmental, or aesthetic improvements for checkpoint and checked baggage areas. 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. After a successful validation through such projects, TSA will consider prototypes for potential transition to acquisition and deployment, qualification for regulated air cargo use, or introduction as products that users can procure through grants programs or purchase with confidence.

Since its inception, the ITF has conducted 46 demonstrations in live operational environments to include several that later materialized into deployments across the country, such as CT and Automated Screening Lanes (ASL). Recently, the ITF completed a demonstration of an X-Ray Diffraction Alarm Resolution unit. The unit was assessed as a secondary AR system in the checkpoint for divested personal property (to include liquids, gels, and aerosols within the 3-1-1 policy) and in the Checked Baggage Resolution Area. The demonstration allowed liquids, gels, and aerosols to be tested without the need to take a trace swab or direct sample by opening the container of the material in question. The X-Ray Diffraction Alarm Resolution unit is located at the Transportation Security Lab in Atlantic City, NJ for continued research and development through DHS S&T.

In addition to demonstrating emerging improvements to various elements of the checkpoint and checked baggage areas, the ITF remains versatile in the technology and requirements space. The task force assists in the prioritization of requirements for new approaches to transportation security and accelerates the development and introduction of new, innovative technologies and improvements to security operations. Regarding stakeholder engagement, the ITF provides industry with access to the airport environment during the technology development and assessment process.

The ITF executes its mission through continuous collaboration and engagement with stakeholders in the aviation security ecosystem and with industry partners to identify solutions, to conduct thorough testing, and to complete field demonstrations. After a successful validation through demonstrations, TSA may consider prototypes for potential transition to acquisition and deployment, qualification for regulated air cargo use, or introduction as products that users can procure through grants programs or can purchase with confidence.

6. Multimodal Transportation Technology

In partnership with surface transportation and air cargo asset operators and industry manufacturers, the Multimodal and Public Capabilities (MPAC) program evaluates advanced technologies and facilitates industry awareness to address identified surface transportation and air cargo security capability gaps. Through formal memoranda of agreement, multimodal partners with representative and higher threat transportation venues are invited to test and evaluate next-generation and emerging technologies in operational transportation conditions and air cargo environments.

7. Surface Security Technology (SST)

As part of TSA's MPAC Division, the SST section stimulates the technology marketplace, evaluates advanced technologies, and facilitates industry awareness to help address identified surface transportation security capability gaps. SST is the co-chair of the DHS and TSA-sponsored Intermodal Transportation Research and Development Working Group. This group serves as a forum for surface-based transportation operators and stakeholders to identify, discuss, and publish security capability gaps within the surface transportation sector. In addition, the Surface Transportation Security Advisory Committee (STSAC) Risk Working Group, comprised of surface transportation industry representatives and other agencies, was formed to gather inputs and feedback from industry stakeholders nationwide, to respond to identified challenges, and to measure and reduce risk by publishing the Security Risk Methodology Catalog to support the purchase of effective security solutions that enhance risk management efforts.

8. Capability Acceptance Process (CAP)

TSA formalized the CAP in 2019 to facilitate receiving capabilities such as TSE and other technologies as donations or bailments from industry stakeholders and partners (i.e., federalized airports and air carriers). The formalized CAP provides an objective and repeatable process to evaluate, accept, and implement requests to offer capabilities. The requests outline the intent of stakeholders and partners to procure, and ultimately to transfer or convey, the capability or TSE to TSA. This process is an option for airport stakeholders and air carriers who may benefit from accelerating procurement and deployment timelines, recapitalizing TSE, and/or enhancing security and the passenger experience.

Since FY 2019, TSA has accepted (or bailed) from airline and airport stakeholders more than 125 pieces of TSE and 3,000 ASL antimicrobial bins. The 125 pieces include more than 90 previously bailed ASLs for a total donation amount of more than $113 million through the first quarter of FY 2023. TSA is currently executing additional CAP projects with 13 donors and is anticipating 2 additional donation projects from two donors in FYs 2023-2024.[16]

9. STSAC

The TSA Modernization Act authorized the establishment of the STSAC to advise, consult with, report to, consider risk-based security approaches, and make recommendations to the Administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security. The committee consists of voting members representing various modes of surface transportation, including passenger and freight rail, mass transit, pipeline, highway, over-the-road bus, school bus, and trucking, as well as nonvoting

[16] Current donors are George Bush Intercontinental Airport, Denver International Airport, Port Authority of New York and New Jersey, American Airlines, Hartfield – Jackson Atlanta International Airport, Private Suite, Charleston International Airport, Miami International Airport, Portland and Charlotte Douglas International Airports, LaGuardia Gateway Partners, Pittsburgh Airport and Delta Airlines with screening technologies that include AIT (40), ASL (6), CPSS (94), CAT (62), WTMD (18), ETD (28), BLS (12), and BPS (61).

advising members from federal entities with regulatory authority over surface transportation. While the STSAC is required by law to meet at least twice a year, with one of those meetings being open to the public, the committee typically meets four times a year with one of these meetings being open to the public.

10. Aviation Security Advisory Committee

The Aviation Security Advisory Committee provides advice to the TSA Administrator on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security. The committee is composed of individual members representing private-sector organizations affected by aviation security requirements. It is focused on recommendations for improvements to aviation security within the four subcommittees of air cargo security, general aviation, perimeter and access control, and security technology. The Aviation Security Advisory Committee, in partnership with TSA, provides a forum for air cargo operators and stakeholders to identify, discuss, and publish security capability gaps within the air cargo sector.

G. Areas for Investment Opportunity (Unconstrained)

The FY 2024 CIP provides Federal government, industry, and Congressional stakeholders with an enterprise view of TSA's technology and infrastructure investments, demonstrating how we are positioned to meet the evolving threat landscape, but within budget constraints.[17] It is in this context that TSA offers its first unconstrained FY 2024 – FY 2028 CIP which reflects the agency's ability to invest in technology solutions if budget constraints were not a factor.

This section lists the array of active, approved procurements that TSA could reasonably accomplish in the FY 2024 – FY 2028 fiscal timeline. It sets the ideal future state of TSA's capital investments required to secure transportation critical infrastructure and takes into account end of service capital investments that require replacement. Failure to replace this aging and outdated aviation equipment carries the risk that TSA will be unable to address the threats to its mission of securing the Nation's transportation systems.

The plan that follows provides a cohesive view of transportation security investments necessary to achieve TSA's strategic priorities within the context of its operational and threat environment. It also describes an ideal future state in which TSA is able to buy down more risk to the transportation sector. The plan serves as TSA's guide when determining and prioritizing future investments to fulfill critical missions.

a. Identity Management

TSA's capabilities within Identity Management (IDM) are constrained by the budget. Currently, roughly 75 percent of the IDM efforts are supported by fee funds, and the remaining efforts are

[17] The Capital Investment Plan is aligned with the National Security Strategy, the National Transportation Security Strategy, the National Cybersecurity Strategy, EO 14028 on Improving the Nation's Cybersecurity, and EO 14008 on Tackling the Climate Crisis at Home and Abroad

funded by base funding. In order to fully maximize the capability of IDM, TSA must ensure the following approved projects are fully funded and operational:

- **CAT-2**: CAT-2 remains a strategic goal of TSA to provide a more convenient passenger experience (e.g., self-service configuration, utilizing mobile driver's licenses (mDL) or Digital Identifiers versus physical IDs) while increasing TSA's security posture at the checkpoint (e.g., utilizing facial recognition for identity verification). The timely procurement and development of the CAT-2 upgrade kits when future enhancements are required will support IDM to reach full operational capability in addition to further expanding CAT-2 enhancements. TSA has the ability to deploy up to 500 new production CAT-2 systems annually based on the resources required to produce, deploy and install these systems without impacting checkpoint operations. Current projected funding levels will allow the CAT program to achieve full operational capability (FOC) in 2049. To accelerate the procurement to 500 production CAT-2 systems over three (3) years, CAT requires an average funding level of $48 million in FYs 2024-2026. This would accelerate FOC from FY 2049 to FY 2027; and
- **mDL:** Currently, Arizona, Maryland, and Colorado mDLs downloaded to Apple iPhones and watches can be used by TSA PreCheck® passengers on CAT-2 units. Many states have expressed interest in developing and deploying their own state-issued mDL. TSA is planning to expand mDL initiatives and mDL readers are planned for incorporation into CAT-2 systems. Digital identification such as mDLs will increase passenger privacy protections through encryption and storage of personal information, enhance airport security effectiveness, and reduce the risk of encountering stolen or counterfeited physical IDs inherent with carrying and using physical identification cards.

b. APS

For TSA to maximize APS capabilities to FOC, several key elements of the program must also occur:

- **CPSS:** The CPSS Program must reach FOC with a one-for-one replacement of the legacy AT systems with the three-dimensional (3D) Computed Tomography (CT) systems. The CPSS Program FOC was therefore set at 2,263 systems that require replacement. As of March 2023, TSA has completed a total of 623 CT installations at airports across the United States for explosives detection. The timeframe to reach FOC depends on actual procurement and deployment quantities each year. TSA has the ability to deploy up to 350 CT systems annually based on average time and resources it takes to deploy system, and the need to minimize disruption to airport operations, preserve passenger throughput, and keep wait times at acceptable levels. Ideally, TSA would reach FOC by FY 2028; however, at the currently funded levels, TSA will achieve FOC in FY 2042. In order to procure and deploy up to TSA's maximum deployment capacity of 350 CT systems/year and reach FOC by FY 2028,

TSA requires an average PC&I funding level of approximately $265 million per year in FYs 2024-FY 2027.

The maturation of the identity management capability will enable TSA to improve the customer experience, required by EO 14058 on Improving Customer Experience, and increase throughput and security at the nation's checkpoints by taking advantage of the automation associated with the Checkpoint CT systems. In the absence of funding to accelerate FOC, TSA will not be able to fully deploy this critical capability for more than a decade, making it more likely for adversaries to exploit the transportation sector to carry out an attack.

IV. Conclusion

TSA maintains a vision for a secure future that it can achieve through investments, partnerships, innovation, and R&D. This future focuses on interconnected Transportation security, continued investment in the TSA workforce, an improved passenger experience, and an elevated security baseline.

The investments identified in the CIP, both in the constrained and unconstrained budget environments, are designed to position TSA to meet the challenges of an evolving threat and transportation landscape. 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 equipped better to identify capital requirements necessary to address identified challenges and risks to transportation security.

Equally important are investments in TSA's most important assets, the dedicated professionals securing our Nation's transportation system. They are vital to ensuring that TSA is able to meet stated challenges. Technology is a major driver behind shifts in TSA's business practices. However, we also need the proper quantity and mix of agile employees, who can adapt to new technologies and circumstances, drive the successful implementation and operation of technological investments and subsequently the success of TSA's mission. Therefore, TSA will ensure a properly staffed workforce that is also equipped with the tools, resources, training, and infrastructure required to conduct frontline functions effectively and efficiently that mitigate risks and outmatch threats.

Appendix

I. Capital Investment Programs (Constrained)

Transportation Security Agency (TSA) operates legacy equipment while evaluating potential replacements in an affordable manner. Transportation Security Equipment (TSE) maintenance, however, remains a large proportion of TSA's capital investments and demands continued resourcing. Figure A1 reflects strictly maintenance contracts and is a subset of the $562M budget for Screening Technology Management which also includes Checkpoint and Checked Baggage technology investments.

Figure A1: TSE Maintenance Funding Profile

TSE Maintenance – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Advanced Imaging Technology (AIT)	$32.9	$32.9	$32.8	$32.9	$32.9	$164.4
Advanced Technology (AT)	$62.0	$62.1	$62.1	$62.0	$62.0	$310.2
Checkpoint Property Security System (CPSS)	$10.4	$10.4	$10.4	$10.4	$10.4	$52.0
Credential Authentication Technology (CAT)	$6.4	$6.4	$6.4	$6.4	$6.4	$32.0
Electronic Baggage Screening Program (EBSP)	$256.2	$256.2	$256.2	$256.2	$256.2	$1,281.0
Explosive Trace Detector (ETD)	$44.4	$44.4	$44.4	$44.4	$44.4	$222.0
Passenger Screening Program Legacy (PSP)	$12.3	$12.5	$12.6	$12.5	$12.5	$62.4
Total TSE Maintenance	**$424.6**	**$424.9**	**$424.9**	**$424.8**	**$424.8**	**$2,124.0**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

A. Vetting and Biometrics

1. Vetting

Vetting Capability Overview: At the TSA, vetting is defined as the process by which data provided by passengers and credentialed populations (e.g., airport, airline, flight crew, air cargo, maritime, Transportation Worker Identification Credential, Hazardous Materials Endorsement, and TSA PreCheck® populations) are 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 configuration of immigration, criminal history, and terrorism checks, depending on the level of access needed. TSA uses evidence-based decision-making and intelligence-driven strategy to understand and

assess the risks posed to the transportation system and to make comprehensive vetting determinations. This approach allows TSA to provide expedited screening for trusted travelers and to focus resources on high-risk and unknown passengers.

Partnerships, resources, and enhanced vetting operations give TSA the ability to ensure the safety and security of people and information in transportation spaces, even as the threat landscape evolves.

Figure A2: Vetting Capability Funding Profile

Vetting Capability - FY 2024 - FY 2028 ($ in millions)						
Program	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Vetting & Credentialing System	$88.6	$88.6	$88.6	$88.6	$88.6	**$443.0**
Secure Flight	$138.9	$144.0	$147.2	$150.0	$152.6	**$732.7**
Total Vetting Capability	**$227.5**	**$232.6**	**$235.8**	**$238.6**	**$241.2**	**$1,175.7**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

i. Vetting and Credentialing System (VCS)

Overview: VCS's mission is to safeguard the Nation's critical modes of transportation and related infrastructure through advanced enrollment, vetting, and credentialing technology, while improving the transportation system user experience. The VCS funding profile, which includes Technology Infrastructure Modernization (TIM) and vetting fees, helped to modernize TSA's vetting and credentialing services by enhancing functionality, by increasing capacity, and by improving the enrollee's vetting and credentialing experience. VCS processes Security Threat Assessments in support of TSA's credentialing programs, which include programs such as the Transportation Worker Identification Credential, TSA PreCheck®, Aviation Worker, Hazardous Materials Endorsement, and Flight Training Student Program, all of which are programs managed by the TSA Enrollment Services and Vetting Programs Office.

Future State: VCS will continue to enhance and achieve the targeted architecture that will consolidate TSA's vetting and credentialing services to serve the mission and stakeholders better. VCS today consists of two FISMA system boundaries that include TIM and VCS, which include applications with similar and duplicated capabilities. For example, each FISMA system has its own infrastructure, external gateway, registration, enrollment, eligibility, vetting, issuance, and redress services. In the future, VCS will integrate the two FISMA systems and applications into a single FISMA boundary by consolidating gateways, services, and other capabilities while implementing best practices.

The consolidated target architecture identifies the necessary steps for improving and simplifying lifecycle costs by leveraging previous investments, by consolidating contracts to support development and operations, and by implementing agile best practices and other proven solutions based on lessons learned. VCS operational efficiency and effectiveness also will improve by maximizing the use of open-source technology, by reducing the use of commercial off-the-shelf technology, and by reusing existing modernized infrastructure and capabilities. The

consolidated target architecture will lower operational cost by: reducing duplication, improving adjudicator user experience by eliminating programs and populations "stovepipe" applications, reducing cost of adaptive maintenance by simplifying data and application architectures, and reducing the cost of adding new vetted and credentialed populations by simplifying data and application architectures.

Figure A3: VCS Funding Profile

VCS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
TIM	$18.8	$18.8	$18.8	$18.8	$18.8	$94.0
Vetting Fees	$69.8	$69.8	$69.8	$69.8	$69.8	$349.0
Total VCS	**$88.6**	**$88.6**	**$88.6**	**$88.6**	**$88.6**	**$443.0**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

ii. Secure Flight Program

Overview: Secure Flight operates a threat-based, intelligence-driven watch list and Trusted Traveler matching capabilities to enhance the security of domestic and international commercial air travel into, out of, within, and overflying the United States, as well as for all U.S.-flagged carriers anywhere in the world. It identifies the appropriate level of physical screening for all passengers and associated baggage. Secure Flight minimizes misidentification of individuals by integrating the DHS redress process and protects personal information from unauthorized disclosure. It prevents international terrorists, domestic terrorists, and Centers for Disease Control and Prevention (CDC)-designated individuals from boarding an aircraft or accessing the sterile area of U.S. airports by effectively identifying those who may pose a threat to aviation security or national security, and by recognizing individuals whom the CDC has prohibited from traveling. The system matching uses the Federal Bureau of Investigation's Terrorist Screening Database, as well as watch lists created under the TSA Administrator's statutory authority ("TSA Watch Lists") to identify known or suspected threats to aviation security. The system matching function also utilizes the CDC no-fly list to identify individuals who are not permitted to travel because of contagion. Secure Flight partners with the TSA PreCheck® team to identify program participants and with U.S. Customs and Border Protection (CBP) to identify other Trusted Travelers. The program also partners with other TSA and Department of Homeland Security (DHS) entities to apply risk-based rules and to identify potential threats to aviation security that are not listed in the Terrorist Screening Database.

Secure Flight reduces the potential security vulnerability of known or suspected terrorists circumventing TSA's vetting and screening processes, enhances vetting analytics and modeling, conducts flight-by-flight risk analysis to inform and drive field operations and planning, improves matching capabilities to address variations in passenger data compared to watch-list information, increases automation to identify potential higher risk passengers, and informs operations and resource planning.

Future State: In the future, Secure Flight will continue to operate with CAT to identify occurrences in which the name screened by Secure Flight does not match the boarding pass and/or passenger identity or travel document presented at checkpoints; and to verify a passenger's vetting status against the Secure Flight database in near real-time (NRT) so that the passenger receives the appropriate screening based on TSA's assessed risk. Secure Flight also will be instrumental in dynamic screening concepts by allowing for risk-based differentiation to be implemented within the security screening equipment. Further vetting and pre-flight risk analysis to drive risk differentiation and operational activities (including Federal Air Marshal information-sharing) will increase screening effectiveness for higher risk passengers.

Secure Flight will maintain currency with evolving technology and transition to an Agile Safe Continuous Integration/Continuous Deployment to enable improved incremental and timely delivery of mission-critical capabilities. The program will continue to: refine watch-list matching, improve vetting algorithms, expand to new aviation populations and data sets, increase efficiencies and intelligence capabilities, and incorporate additional risk factors beyond direct watch list and Trusted Traveler matching. These changes will increase the automation of the vetting engine and will improve high-risk passenger rules and watch-list matches, while significantly decreasing false positives and minimizing the risk for potential false negatives.

The planned system improvements will strengthen the Secure Flight tools utilized by the National Transportation Vetting Center. This system and operations maturation will include built-in, real-time data analytics capability to drive operational planning and responses and to provide feedback to the intelligence community. It also will provide a platform for real-time reporting and passenger information metrics across the aviation system.

Figure A4: Secure Flight Funding Profile

Secure Flight – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Secure Flight	$136.4	$141.5	$144.7	$147.5	$150.1	$720.2
Traveler Redress Inquiry Program (TRIP)	$2.5	$2.5	$2.5	$2.5	$2.5	$12.5
Total	**$138.9**	**$144.0**	**$147.2**	**$150.0**	**$152.6**	**$732.7**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

Future of the Vetting Capability: TSA aims to make technological and functional process improvements to increase the speed and accuracy of vetting results and to better understand and assess the risks posed to the transportation system. These efforts include:

- Enhancing the credential holder and passenger experience during enrollment and travel reservation;
- Building a lower touch and seamless travel experience from curb to gate, beginning with enrollment;

- Ensuring that enrollment capabilities are aligned to leading standards and processes for identity assurance for both physical and digital credentials;
- Exploring the feasibility of remote enrollment to complement existing capabilities for credential programs. This includes assessment of remote photo capture and back to the source capabilities;
- Improving and expanding identity proofing standards using automated tools that minimize manual errors, while also streamlining the level of government and applicant interactions. TSA is also working to establish identification documents (ID) proofing standards for physical and digital IDs by leveraging National Institute of Standards and Technology standards as the basis for standardization and to determine key success factors for proofing applicant identity credentials back to the issuing source. These standards will increase TSA's confidence that the issuing source conducts due diligence to rule out fraud prior to issuing a physical/digital credential. Furthermore, IDM stood up the Acceptable Forms of ID Working Group under the IDM Capability Integration Council, which established criteria and a supporting evaluation methodology for TSA Acceptable Forms of ID. This work will address critical identity acceptance and verification vulnerabilities associated with the current Acceptable ID list;
- Evolving vetting capabilities using a risk-based approach to conduct data-driven applicant screening and assessments, using technological and process improvements to enhance vetting speed and accuracy. The vetting process was further enhanced through checkpoint modernization and the incorporation of CBP system linkage to streamline identity verification resolutions with the incorporation of additional data sets. TSA is also exploring enhancements to the Identity Verification Call Center to streamline identity verification resolutions at the checkpoint; and
- Maturing its risk-based approach to increase the use of biometrics screening, to improve confidence in security verification, and to minimize the risk of adversary manipulation through priority investments in the IDM portfolio focused on: CAT-2, digital identity technology, and identity proofing and enrollment. Implementation of IDM capabilities requires systems integration, biometric system improvements, data analytics and algorithm development, cybersecurity, and standardization and requirements. These activities are investments in IDM capabilities that will ensure a safe and secure TSA checkpoint as technology continues advancing and as adversaries find new methods of attack.

2. Identity Management

IDM Capability Overview: In April 2018, CBP and TSA signed the Joint TSA-CBP Policy on the Use of Biometrics, committing to exploring the use of biometric facial recognition technology. In October 2018, TSA published its Biometrics Roadmap to outline four strategic goals that it will pursue to deploy biometric facial recognition technology in the field:

- Partner with CBP on the use of biometric identification technology for international travelers at TSA security screening checkpoints;

- Operationalize biometrics for identity verification for TSA PreCheck® travelers;
- Expand biometric identification technology to additional domestic travelers; and
- Develop supporting infrastructure for biometric solutions.

Building on the success of the TSA Biometrics Roadmap, TSA released the TSA IDM Roadmap in March 2022. The document articulates a comprehensive end-to-end strategy for what IDM means for TSA and chronicles the next iteration of TSA's thinking on biometrics and digital identity. It is critical to TSA's mission as it ensures the right people have access to the right transportation infrastructure areas at the right time. The IDM Roadmap outlines TSA's vision to transform the IDM lifecycle through four main goals:

- Enhancing the credential holder and passenger experience during enrollment and reservation;
- Continuing to expand and evolve standards for identity proofing to support future vetting and verification activities;
- Continuing to evolve the vetting capability in response to new threats, policies, and technologies; and
- Supporting appropriate identity verification activities across TSA.

IDM at TSA is the continuous process of ensuring the right people have the right access, physically and virtually, at the right times, for the right reasons. IDM is responsible for ensuring the integration of identity-related activities and prioritizing resources across TSA through a united strategy that enhances the proofing and enrollment; vetting; and identity verification of populations throughout the aviation security enterprise. TSA is working to ensure that enrollment and proofing capabilities align with leading standards and processes for identity assurance to strengthen vetting outcomes and identity verification. Since publishing the Biometrics Roadmap, TSA continues evolving and building its perspective on IDM into a more formalized and integrated capability across the enterprise, with the addition of the Identity Management Roadmap.

Identity proofing and enrollment is the act of confirming that someone is who they claim to be per identity assurance leading practices. The advent of digital identity provides an opportunity to assess how technology can support TSA's identity proofing and enrollment capabilities while informing its vetting and identity verification processes. As TSA implements new proofing solutions, it will need to invest in technologies and tools that support its efforts to perform identity proofing across various airport touchpoints and populations.

Figure A5: IDM Funding Profile

IDM - FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
CAT	$14.6	$16.4	$17.2	$18.9	$20.0	$87.1
Identity Investment	$2.3	$2.6	$2.6	$2.6	$2.6	$12.7
Boarding Pass Scanner (BPS)	$0.9	$0.9	$0.9	$0.9	$0.9	$4.5
Subtotal O&S	**$17.8**	**$19.9**	**$20.7**	**$22.4**	**$23.5**	**$104.3**
CAT	$11.0	$9.3	$8.4	$6.8	$5.7	$41.2
Subtotal PC&I	**$11.0**	**$9.3**	**$8.4**	**$6.8**	**$5.7**	**$41.2**
Total	**$28.8**	**$29.2**	**$29.1**	**$29.2**	**$29.2**	**$145.5**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

The following transportation security equipment (TSE) solutions are funded for TSA's IDM capabilities. TSA also is investing in additional capabilities to advance the use of IDM in the future.

i. Biometric Technology (Expanding 1:n Facial Recognition Solution)

Overview: Biometric technology enables verification of passenger 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). As part of the continuation of TSA's 1:n integration with CBP, TSA developed the Touchless TSA PreCheck® solution to create a secure link between TSA's Secure Flight vetting system and CBP's biometric Travel Verification Service. The link allows TSA to identify passengers and their corresponding vetting status at the TSA checkpoint using facial identification technology. Biometrics can enable TSA to automate part of the current manual procedures and allows TSOs to use their training and experience to focus more on anomalies and error resolution. As a result of the COVID-19 environment, TSA has evaluated ways to automate the identity verification process for travelers through the use of biometric technology and digital identity. Using this technology supports TSA's focus on reducing points of contact for travelers and paves the way for a more seamless travel experience while protecting passenger privacy and civil liberties.

Future State: TSA's biometric technology programs have helped balance technical developments and usability requirements to inform long-term requirements development. Program development has shown the potential for identity technology to enhance security effectiveness, to improve operational efficiency, and to yield a more streamlined and touchless passenger experience. Biometric recognition capabilities will improve the performance and security of TSA operations by increasing assurance of traveler identity.

In the future, TSA must consider innovative solutions that allow IDM improvements, while mitigating potential risks that these new technologies may introduce to our transportation system. TSA is continuing to work closely with CBP and Delta Air Lines to advance piloting of the TSA PreCheck® Touchless Identity Solution at Detroit Metropolitan Wayne County Airport (DTW)

and Hartsfield-Jackson Atlanta International Airport (ATL) airports. Checkpoint prototypes in the field will be replaced by 1:n-enabled CAT-2 units pending successful integration and testing. TSA is also working to coordinate internally and other stakeholders on multiple airline/airport-led biometric innovation initiatives related to biometric bag drop initiatives. TSA will continue improving user experiences through testing solutions that increase the level of self-service and front-end tools available or when exploring biometric identity verification solutions, making customer success and safety a consistent priority.

ii. CAT

Overview: CAT provides the primary means for authenticating ID security features that passengers present to TSOs before they enter the passenger screening checkpoint and for verifying their Secure Flight vetting status and flight reservation information.

Figure A6: CAT

CAT closes current checkpoint security gaps by improving the ID inspection and by confirming passengers' vetting status. The CAT program enhances TSA's ability to verify passenger ID authenticity, flight reservation status, and Secure Flight screening status. It also enhances the passenger experience with safer self-service configurations and eliminates the need to present a boarding pass in most instances.

As of December 2022, the fleet consists of approximately 2,054 CAT systems operating across 226 facilities (airports/training and testing centers). The CAT program reached FOC with 1,520 units deployed in the first quarter of FY 2022.

Future State: The CAT program re-baselined in FY 2022 to increase the FOC quantity and to implement requirements supporting a self-service version of the current CAT system (CAT-2), including a camera for 1:1 facial biometric verification and authentication of mobile driver licenses/digital IDs. The program is going through an open competition to find vendors that can meet the new requirements and is also upgrading the current CAT systems to CAT-2 capabilities. CAT-2 upgrades will be built on the existing CAT infrastructure. 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.

Figure A7: CAT-2

In 2022, TSA began conducting expanded field pilots of CAT-2 capability with upgraded CAT units. The upgraded units feature the same CAT-2 functionalities, as well as a digital ID reader, updated user interface, and form factor enhancements including a new podium and space for additional processing power.

Figure A8: CAT Funding Profile

CAT FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
CAT	$14.6	$16.4	$17.2	$18.9	$20.0	$87.1
Subtotal O&S	**$14.6**	**$16.4**	**$17.2**	**$18.9**	**$20.0**	**$87.1**
CAT	$11.0	$9.3	$8.4	$6.8	$5.7	$41.2
Subtotal PC&I	**$11.0**	**$9.3**	**$8.4**	**$6.8**	**$5.7**	**$41.2**
Total CAT	**$25.6**	**$25.7**	**$25.6**	**$25.7**	**$25.7**	**$128.3**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

iii. Boarding Pass Scanner (BPS)

Overview: A BPS reads a passenger's boarding pass and displays the passenger's name, flight information, and screening status to the Travel Document Checker (TDC). The TDC uses this information to ensure that passengers are routed appropriately in the security screening checkpoint. BPS units currently are deployed to every TDC, but at TDCs with CAT, they are only used for passengers not required to have an ID (e.g., young children) and in other limited circumstances.

Figure A9: BPS

Future State: BPSs will continue to be the primary screening system for passengers who are not required to present identification as a system for proofing/enrollment, vetting, and identity verification. Eventually, BPS will be incorporated into CAT-2 allowing for a more efficient identify authentication process. The BPS also will be the primary screening system when CAT is unavailable for use. Approximately 3,050 BPSs are available for use (as of December 2022).

Figure A10: BPS Funding Profile

BPS Funding Profile FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
BPS	$0.9	$0.9	$0.9	$0.9	$0.9	$4.5
Total BPS	**$0.9**	**$0.9**	**$0.9**	**$0.9**	**$0.9**	**$4.5**
FY 2024 reflects the President's Budget, and FY 2025 – FY 2028 are estimated amounts.						

Future of the IDM Capability: TSA is evolving and managing a cohesive identity management ecosystem within TSA and with its partners that supports improving security effectiveness, the human experience, and operational efficiency in support of current and future Federal requirements such as REAL ID. TSA will continue to improve traveler experiences by exploring and testing self-service identity verification solutions, as well as digital identity

capabilities, to enable TSA to better meet the challenges of evolving security threats, rising air travel volumes, resource constraints, and limits on operational footprint. IDM will focus on creating digital identity solutions that ensure TSA is equipped to integrate emerging technology at the TSA checkpoint. Future developments in projects include CAT-2 upgrades, AutoCAT/eGate developments, digital identity capabilities, 1:n implementation within the TSA PreCheck® – Touchless Identity Solution, and Bag Drop Pilots.

- **CAT-2:** CAT-2 is an enhancement to the currently fielded ID authentication solution. This solution addresses the need to more securely verify an individual's identity by performing facial recognition from the image on a physical or digital ID to the person presenting the ID at the security checkpoint. In 2022, TSA began conducting expanded field pilots with upgraded CAT-2 units. The upgraded units feature the same CAT-2 functionalities, as well as a digital ID reader, updated user interface, and form factor enhancements including a new podium and space for additional processing power. CAT-2 automates the identity verification function that TSA officers normally perform manually, using the same physical credentials that TSA has always accepted. Passenger participation is voluntary and if a passenger chooses not to participate in a pilot, they can have their identity verified manually instead.
- **AutoCAT/eGate:** TSA is exploring an automated gate variant of the CAT-2, called AutoCAT. AutoCAT includes self-service CAT-2 functionalities with the addition of an electronic gate (e-gate) for positive passenger control. This solution has the potential to further automate the identity verification process and reduce physical contact between the TSA officer and passengers. It also reduces the level of staffing required to oversee identity screening operations, thus allowing TSA to re-allocate valuable resources to other pressing security tasks (e.g., baggage screening, alarm resolution). While a completed AutoCAT would provide a touchless identity verification experience, there still remains testing and research to do before a product can be piloted.
- **Digital Identity (DI):** TSA is engaging with states and private sectors to integrate digital identity capabilities in its existing identity verification platforms, including the integration of mDL. TSA has worked to upgrade its existing ID verification systems (CAT-1) with a camera and mDL scanning capabilities. The DI/mDL efforts impact many stakeholders and require cooperation between all of them, which makes this effort particularly challenging. Continued research is important to continue to keep these efforts up to industry standards.
- **TSA PreCheck® – Touchless Identity Solution**: TSA began piloting the TSA PreCheck® Touchless Identity Solution at DTW checkpoint in March 2021. In November 2021, the pilot was expanded to support the baggage drop touchpoint at ATL. In May 2022, the pilot launched at the ATL checkpoint. In the coming years, TSA and CBP plan to scale the TSA PreCheck® Touchless Identity Solution to provide a token-less curb-to-gate experience across several airports and airlines within the U.S. This travel experience will be characterized by streamlined processing, minimized wait times, fewer travel documents, increased security, decreased stress, and fewer points of contact between passengers and TSA officers. Part of this experience includes the option to use Touchless Identity Solution to complete a baggage drop prior to entering the sterile area of the airport. The solution has been piloted in ATL and there are plans to expand the

feature to LaGuardia International Airport and Los Angeles International Airport (LAX) in 2023.

TSA's current capabilities to verify the identity and obtain the risk level of travelers at the TSA checkpoint are limited. TSA will invest in the following opportunities to create the checkpoint of the future:

- Biometric technology through enhancements to systems and collection of biometrics to verify identity at the checkpoint;
- R&D to develop back-end architecture to enable biometric data;
- Remote, self-enrolled digital identity standards and solutions to enable touchless identity enrollment and proofing that can be trusted for transportation security purposes; and
- DI solutions that allow digital identities and mDL to be accepted at the checkpoint.

TSA has made immense developments in its priority projects and requires continual support to make the necessary mission progress at the speed of agency need.

B. Threat Detection System-Of-Systems

1. APS

APS Capability Overview: The APS capability aims to enhance the security effectiveness and operational efficiency of TSA's APS functions through means of automation, integration, and connection. The primary objectives of the APS capability include mitigating evolving threats and capability gaps present at the checkpoint, improving the passenger experience, enhancing screening detection, increasing throughput, and enabling screening automation.

APS highlights several functional areas that allow TSA both to mature the capability and to meet developmental objectives at security checkpoints nationwide. The APS and Checkpoint Property Screening Capability Maturation Roadmap guides the development of these functional areas, depicting current and future efforts required to strengthen carry-on screening detection capabilities. Through the implementation of the CPSS Program, TSA seeks to develop, acquire, and implement dynamic material and nonmaterial-based solutions to enhance checkpoint and aviation security further.

APS functional areas include:

- **Move:** Improving divestiture experience for passengers and reducing physical burden for TSOs transporting bins.
- **Detect:** Enhancing detection capabilities with the introduction of prohibited items algorithms and advanced explosives algorithms, allowing additional items (e.g., empty water bottles) through the checkpoint.

- **Display:** Streamlining system usability with the use of standardized scanner displays and optimizing operational efficiency with a planned Image on Alarm Only concept of operations.
- **Connect:** Empowering risk-based screening through connecting passenger data with APS.

Figure A11: APS Capability Funding Profile

APS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
APS	$0.6	$0.6	$0.6	$0.6	$0.6	$3.0
CPSS O&S	$56.4	$56.7	$56.7	$56.7	$56.7	$283.2
AT	$72.9	$72.9	$72.9	$72.9	$72.9	$364.5
Subtotal O&S	**$129.9**	**$130.2**	**$130.2**	**$130.2**	**$130.2**	**$650.7**
CPSS PC&I	$70.4	$70.4	$70.4	$70.4	$70.4	$352.0
Subtotal PC&I	**$70.4**	**$70.4**	**$70.4**	**$70.4**	**$70.4**	**$352.0**
Total APS	**$200.3**	**$200.6**	**$200.6**	**$200.6**	**$200.6**	**$1,002.7**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

i. Computed Tomography (CT)

Overview: Previous DHS R&D efforts and more than 22 years of using CT technology to screen checked baggage effectively and efficiently have suggested that the CT systems are the most impactful technology available today to address rapidly evolving threats and security vulnerabilities at airport checkpoints. CT technology automates explosive items detection by eliminating the variability introduced by human screeners and enables stronger threat detection by providing 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. With the CT's enhanced imaging capabilities, TSA anticipates eventually eliminating the need to remove electronics, laptops, and liquids, aerosols, and gels from carry-on bags, improving the passenger experience.

Figure A12: CT

TSA currently operates 45 pilot CT units across the 4 CT vendors to develop and demonstrate new capabilities developed under APS. The range of capabilities fall under the focus areas of MOVE, DETECT, DISPLAY and CONNECT. Specific examples of recent developments include advanced explosives algorithms, Prohibited Items (PI) algorithms, Remote Screening/Networking, and integration of CTs with Automated Screening Lanes (ASL).

The pilot units for Smiths Detection paved the way for procurement of the 300 Advanced Technology (AT)/CT units as a project under the AT Program. TSA has completed a total of 534 CT installations at airports across the United States for explosives detection. An additional 15 CT systems have been deployed to various laboratory, training, and vendor facilities. In alignment with the APS portfolio, CPSS has been added to enable the enhancement of security effectiveness and operational efficiency of TSA's accessible property screening functions through means of automation, integration, and connection. CPSS is designed to mitigate evolving threats and capability gaps present at the checkpoint. The primary objective for the CPSS Program is to develop, acquire, and implement dynamic materiel and non-materiel based, modular capabilities that will enhance aviation security while improving the passenger experience at the checkpoint.

Future State: TSA seeks to develop and demonstrate new CT capabilities in support of and realized through the CPSS program. The range of capabilities falls under AT/CT, CPSS base, CPSS mid-size, and CPSS full-size. Specific examples of recent developments include advanced explosives algorithms, prohibited items algorithms, and remote screening/networking.

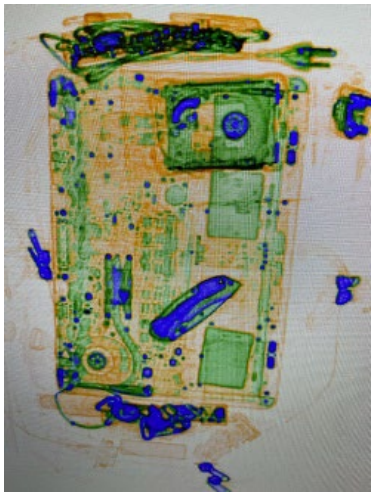


Figure A13: CT Imagery

TSA is using an incremental acquisition strategy to deploy enhanced checkpoint screening capabilities throughout the life of the program. These capabilities are driven by TSA R&D activities as well as by industry readiness. The CPSS Program is executing Increment 1 and is in the planning stages for Increment 2:

- **CPSS Increment 1 (FY 2021 – FY 2025)**: Procure and deploy CPSS configurations (base, mid- and full-size) with an advanced threat detection standard and STIP compatibility; and
- **CPSS Increment 2 (FY 2024 –FY 2027)**: Procure and deploy CPSS configurations with an advanced threat detection standard and STIP connection (networked).

Key activities include:

- **Explosives & Non-Explosive Prohibited Items Algorithm Development for CT:** In alignment with the announcement for the CPSS Capabilities Maturation Roadmap and incremental CPSS advances, TSA is pursuing advancements in the explosives detection capabilities of CT scanners as well as detection of non-explosive prohibited items using machine-learning algorithms to enable a "View on Alarm Only" concept of operations;
    - TSA piloted PI algorithms in an effort to move to Image on Alarm Only (IOAO) that were certified in Q2 FY23.
- **Enhancing CPSS Network Capabilities:** Primarily involves the maturation of remote screening at the checkpoint, a capability that will relocate TSOs from checkpoint lanes to

a remote location, thus offering the potential for staffing optimization, improvements to operational efficiency, and an increase in social distancing of TSOs and the traveling public;

  - TSA is currently piloting remote screening/cross-lane screening capabilities at ATL, MIA, EWR, and IAH to improve utilization of current resources and determine options for staffing optimization.

- **Two new concepts of operations:** Focus on the primary screening of oversized liquids/gels/aerosols (LGA) utilizing improved detection capabilities at Tampa International Airport (TPA), MIA, IAH, Albany International Airport (ALB), Bellingham International Airport (BLI), and Peoria International Airport (PIA); and
- **Reduced Footprint CT:** TSA has installed the first system for data collection in Las Vegas Airport (LAS). Data collection will be done to provide analysis to inform and to develop reduced-size CTs for checkpoints unable to support current CT configurations.

Figure A14: CPSS Mid-Size

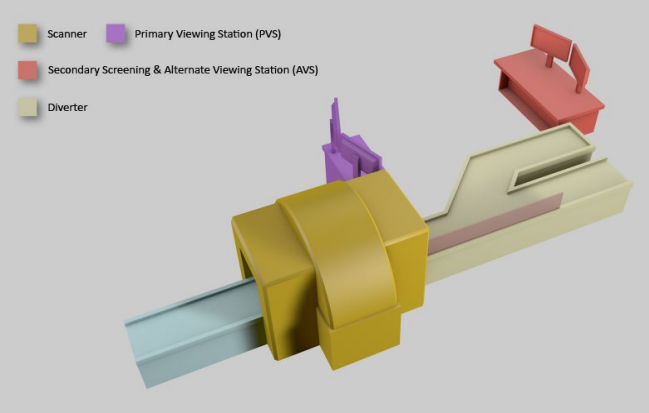


Figure A15: CPSS Full-Size

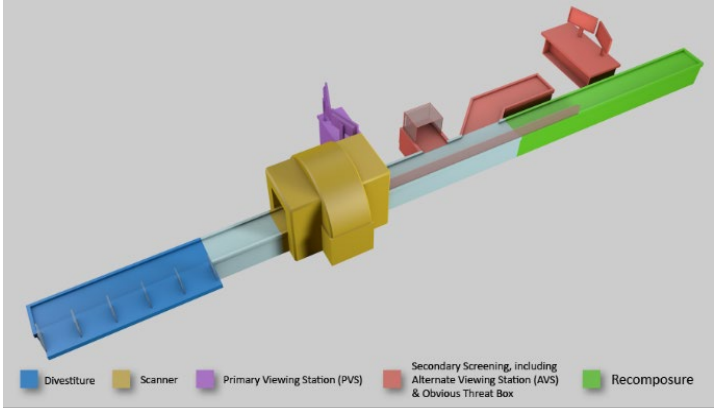


Figure A16: CPSS Funding Profile

CPSS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
CPSS O&S	$56.4	$56.7	$56.7	$56.7	$56.7	$283.2
CPSS PC&I	$70.4	$70.4	$70.4	$70.4	$70.4	$352.0
Total CPSS	**$126.8**	**$127.1**	**$127.1**	**$127.1**	**$127.1**	**$635.2**
FY 2024 reflects the FY 2024 President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

ii. Advanced Technology X-rays

Overview: AT X-ray systems detect threats concealed in passengers' accessible property upon entrance to the screening checkpoint. ASL are a property-handling system integrated into an

existing AT system to mitigate checkpoint security vulnerabilities, to improve checkpoint efficiency and throughput, and to reduce the number of misdirected bags identified for additional screening. TSA partnered with airlines and airports to install ASL units at high-traffic security screening checkpoints and to connect them to existing AT2 systems. TSA never procured ASLs, and no longer accepts ASLs as donations; however, TSA assumes costs for maintenance of these donated systems after warranties expire.

Future State: There are approximately 1,955 AT standalone systems deployed to the field and 236 AT systems integrated with ASLs (as of December 2022). The program has reached FOC. TSA will continue to deploy enhanced algorithm capabilities to the remaining AT and AT/ASL systems as the fleet will be replaced gradually as CT systems are deployed to the field.

Figure A17: AT

Figure A18: AT Funding Profile

AT - FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Advanced Technology (AT)	$72.9	$72.9	$72.9	$72.9	$72.9	$364.5
Total AT	**$72.9**	**$72.9**	**$72.9**	**$72.9**	**$72.9**	**$364.5**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

Future of the APS capability: Operational efficiency is the capacity of systems (technology and process) to maintain security effectiveness by streamlining core processes and developing and implementing screening solutions in the most cost-effective manner possible. As TSA screens and processes an average of 1.8 million passengers every day across the United States, investment in CPSS is targeted to expedite carry-on baggage processing times and passenger throughput. TSA's APS capability has therefore focused future efforts to address the following:

- **Network Connectivity:** In its efforts to develop an integrated, networked security screening environment, TSA intends to use network connectivity as a means to securely exchange data between TSEs, the enterprise, and external databases. The integration of CPSS with other TSE will also enable Risk-Based Security as CPSS could have a means for pulling passenger risk information. This information could be passed along by other TSEs and retrieved from external databases (i.e., Secure Flight). Additionally, one of the goals of the network connectivity program is to gain the ability to push firmware updates and perform remote diagnostics over the network rather than requiring in-person visits from field technicians. Through remote monitoring and maintenance, TSA can be more readily notified of performance issues or risks from fielded systems.
- **Remote Screening:** The networking of TSE at the checkpoint will introduce secure remote screening that will enable detection beyond the checkpoint. Operators will be able to screen and clear carry-on baggage remotely through a networked CPSS

configuration, thus potentially improving overall checkpoint throughput and reducing the cognitive burden on the TSOs at the checkpoint.

- **False Alarm Rates:** By developing more advanced detection algorithms for both explosives and non-explosive prohibited items, TSA will continue to enhance security effectiveness and reduce false alarm rates, as well as shift to a future-state of risk-based security screening that enables an improved passenger experience. Current screening procedures, as a result of existing checkpoint screening detection standards, require passengers to remove laptops and all LGAs from their bags. With enhanced detection algorithms, CPSS will detect a wider range of explosive threats at smaller threat masses, as well as non-explosive prohibited items (PI). These detection enhancements will further improve the passenger experience by reducing the types of articles required for removal from carry-on baggage, and pat-downs that will enhance efficiencies in TSA's data-driven screening process.
- **Automated Detection:** CPSS will reduce complexity in APS by automating detection of threats in a manner that maintains an operationally acceptable false alarm rate. Future threat detection algorithms will also aim to produce an IOAO Concept of Operations. Under IOAO, the system provides an image to the Primary Viewing Station (PVS) operator only when the algorithm determines there is an item of interest in the bag that meets the threat criteria, whether an explosive or non-explosive PIs.

CPSS will also move to IOAO screening, relying on detection algorithms to allow scanners to detect more threats automatically with the goal that only alarmed bag images need to be examined by the TSO. If IOAO is enabled, the scanner is capable of clearing an item in primary screening when the explosive and non-explosive prohibited items algorithms do not detect any threats present. In this mode, only images with possible threats detected are sent to the primary screening image queue for review by a TSO. Working collaboratively with the automated conveyance function of CPSS, eventually carry-on baggage that receives an alarm during the initial primary screening could be automatically diverted to secondary screening without the PVS operator seeing the image.

2. Alarm Resolution (AR)

AR Capability Overview: TSA uses primary and secondary screening countermeasures at airport checkpoints and for checked baggage. When primary screening devices detect a potential threat, an alarm is generated. In secondary screening, checkpoint and checked baggage include AR and Advanced Alarm Resolution (AAR) operations to determine whether the person or property can be allowed into the secure area of the airport. The current focus of AR is to advance AR capabilities to effectively identify, analyze, verify, and resolve alarms from primary screening, beginning with checkpoint APS and then expanding to the rest of checkpoint and checked baggage. 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 (networking) in order to improve data sharing, fleet maintenance, cybersecurity monitoring, and algorithm development.

Figure A19: AR Capability Funding Profile

Alarm Resolution – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
ETD	$46.8	$46.8	$46.8	$46.8	$46.8	$234.0
BLS	$2.5	$2.2	$2.2	$2.3	$2.2	$11.4
Chemical Analysis Device (CAD)	$0.8	$0.8	$0.8	$0.8	$0.8	$4.0
Alarm Resolution (O&S, STM)	$0.6	$0.6	$0.6	$0.6	$0.6	$3.0
Subtotal O&S	**$50.7**	**$50.4**	**$50.4**	**$50.5**	**$50.4**	**$252.4**
Emerging Alarm Resolution Technologies	$3.0	$3.0	$3.0	$3.0	$3.0	$15.0
Subtotal R&D	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$15.0**
Total AR	**$53.7**	**$53.4**	**$53.4**	**$53.5**	**$53.4**	**$267.4**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

TSA is developing the following TSE solutions to evolve AR capabilities and to create the checkpoint of the future:

i. ETD

Overview: ETD is TSA's most relied-upon AR capability. The high sensitivity, of ETD systems, enable Transportation Security Officers to perform fast and accurate screening for explosive trace from a wide range of threats on a variety of surfaces. ETDs are used to screen passengers, their accessible property and checked baggage.

The ETD fleet has reached FOC and consists of approximately 5,848 deployed units (as of December 5, 2022). The current ETD fleet technology is based on ion mobility spectrometry, a Track 2 technology.

Figure A20: ETD

The ETD program is executing software and hardware component upgrades for fielded systems to address additional threats that are currently identified in primary screening. These enhancements will continue as new AR technologies are developed to recapitalize the ETD fleet. The current fleet is beginning to experience issues with parts obsolescence and failing systems, and OEMs are struggling to meet current detection requirements.

Future State: In support of a future AR Program, TSA will require a next generation replacement capability, Technology Track Resolution, to meet additional emerging threats and to replace the current fleet, which is approaching end of life.

Figure A21: ETD Funding Profile

ETD – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
ETD	$46.8	$46.8	$46.8	$46.8	$46.8	$234.0
Total ETD	**$46.8**	**$46.8**	**$46.8**	**$46.8**	**$46.8**	**$234.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

ii. BLS

Overview: A BLS is a confirmatory technology that differentiates dangerous liquids and compounds from common, benign substances carried in clear bottles by passengers during the checkpoint screening process. Approximately 1,620 BLS systems (as of December 2022) are deployed to the field. BLSs are part of the PSP legacy. TSA is procuring BLSs periodically to meet airport growth, expansion, and safety stock needs.

Figure A22: BLS

Future State: In support of a future AR Program, a next generation replacement capability will be required to meet Detection Standard 3.0 or higher, and to accommodate additional bottle types. TSA is testing the CEIA EMA-MS model to determine its capability in meeting Detection Standard 2.3 without modifying hardware or software. Proven successful, TSA will seek funding to replace the Smith Detector Model Responder in the field with the model EMA-MS in FY 2024 and FY 2025.

Figure A23: BLS Funding Profile

BLS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
BLS	$2.5	$2.2	$2.2	$2.3	$2.2	$11.4
Total Alarm Resolution	**$2.5**	**$2.2**	**$2.2**	**$2.3**	**$2.2**	**$11.4**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

iii. Emerging Technologies

Through R&D, TSA leveraged a request for information to inform the draft requirements and release of a request for proposal in FY 2021. It initiated technical demonstrations and iterative development of the two most promising confirmatory solutions submitted by industry.

Figure A24: Emerging Technologies

This R&D effort is a necessary pathway to excel in industry development and assessment of next-generation AR technologies so that TSA can mitigate credible threats to aviation effectively.

The solicitation identified numerous systems at varying Technology Readiness Levels (TRL). Demonstrations of selected submissions will be conducted at federalized laboratories and selected airports. Because of funding constraints, R&D will be executed in two stages, Track 1 and Track 2, identified below:

- Track 1 will be focused on high-TRL solutions. Available funds are expected initially to allow TSA to evaluate only two confirmatory technologies, such as bulk detection, starting in FY 2022 and continuing through FY 2024. FY 2023 funding will support field assessments at airports to demonstrate a system's ability to meet operational requirements in its intended environment. To minimize the duration of the capability gaps, requirements documents, such as the concept of operations and operational requirements document, will be developed during Track 1 with the goal of achieving Acquisition Decision Event milestone 2A in FY 2024.
- Track 2 will be focused on developing mid-TRL solutions that will address critical capability gaps not addressed by Track 1 and is planned to start in FY 2025, when TSA expects to evaluate at least one vendor from FY 2025 to FY 2027. The $3 million in the FY 2023 Budget is for the Track 1 R&D development.

Figure A25: Emerging Technologies Funding Profile

Emerging Technologies – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Alarm Resolution (O&S, Screening Technology Maintenance)	$0.6	$0.6	$0.6	$0.6	$0.6	$3.0
Subtotal O&S	**$0.6**	**$0.6**	**$0.6**	**$0.6**	**$0.6**	**$3.0**
Emerging Alarm Resolution Technologies	$3.0	$3.0	$3.0	$3.0	$3.0	$15.0
Subtotal R&D	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$15.0**
Total Emerging Technologies	**$3.6**	**$3.6**	**$3.6**	**$3.6**	**$3.6**	**$18.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

Future of the AR Capability: The future of AR is outlined by the AR Roadmap, which highlights the technologies, process, and capabilities required to take AR from the current state to the next-generation capability. TSA looks to advance screening methods to identify and discriminate alarmed items in containers or concealments that do not allow access for sampling. Contactless AR is a desired capability in which TSE identifies and analyzes alarmed material with no additional procedures or TSE needed to clear the alarm. To increase efficiencies, AR will seek to implement automation, reduce labor-intensive processes, and simplify operations in part by improving procedures and utilizing new technology that will identify more benign materials and thus result in the confiscation of less passenger items that are commonly seen in the normal stream-of-commerce and reduce overall passenger wait times that can be linked to

cumbersome Access Request and Automated Access Request processes related to known technology capability gaps.

AR also will look to demonstrate networking capabilities, using open architecture concepts where possible, to facilitate real-time detection algorithm switching, remote software updates and cyber monitoring, and the timely sharing of AR data through local airport networks and/or STIP. NRT AR data sharing will provide TSA timely insight of primary screening false alarm rates, to improve screening effectiveness, and to lower primary screening false-alarm rates via such means as manual technical analysis, TSE machine learning and/or artificial intelligence. AR initially will demonstrate the capability to share resolution data directly with technologies that are part of the CPSS program to inform improvements in primary screening false alarm rates and will support adding AR TSE to the Digital Imaging and Communications in Security v3.0 standard.

3. On-Person Screening

On-Person Screening (OPS) Capability Overview: TSA's OPS capability ensures the safety of commercial aviation by screening airline passengers and aviation workers. OPS focuses on improving advanced imaging technology (AIT) systems, Enhanced Metal Detectors (EMD), pat-down procedures, and other emerging OPS capabilities. AIT systems are TSA's best OPS detection technology; however, many have been deployed for almost a decade and take up significant space in the checkpoint. The AIT program aims to achieve increased throughput and enhanced detection standards to eliminate most checkpoint bottlenecks associated with passenger screening. To enable AIT screening of a larger share of passengers, TSA will conduct R&D and will work with vendors to develop and acquire faster and smaller next-generation AIT systems.

In the meantime, TSA will explore and invest in opportunities that improve security effectiveness by enhancing detection performance, by reducing false alarm rates, by extending the fleet useful life, and by conducting R&D activities for potential next-generation AIT alternatives. These activities include:

- Retrofit current fleet with High Definition (HD)-AIT wideband kit and algorithm upgrades;
- Explore nonmetallic EMD replacements;
- Test and Deploy Gender-Neutral Screening (included in the FY 2022 and FY 2023 budgets); and
- Introduce open architecture concepts such as DICOS and OPSL to enable long-term capabilities.

TSA will seek to invest in new technology that can increase passenger throughput, can meet current detection standards, and can connect to a secure network. TSA also will invest in R&D for next-generation OPS technologies that can: achieve screening at speed, discriminate between different materials, scan shoes on passenger, and promote a more contactless checkpoint.

Figure A26: OPS Capability Funding Profile

On-Person Screening (OPS) – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
AIT	$38.5	$38.7	$38.7	$38.7	$38.7	$193.3
PSP Legacy Walk-Through Metal Detectors (WTMD)	$3.3	$3.4	$3.4	$3.4	$3.5	$17.0
On-Person Detection/Next Gen AIT (O&S, Non Investment)	$1.0	$1.0	$1.0	$1.0	$1.0	$5.0
Subtotal O&S	**$42.8**	**$43.1**	**$43.1**	**$43.1**	**$43.2**	**$215.3**
On-Person Detection/Next Gen AIT	$5.0	$5.0	$5.0	$5.0	$5.0	$25.0
Subtotal R&D	**$5.0**	**$5.0**	**$5.0**	**$5.0**	**$5.0**	**$25.0**
Total On-Person Screening (OPS)	**$47.8**	**$48.1**	**$48.1**	**$48.1**	**$48.2**	**$240.3**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

TSA is developing the following TSE solutions to evolve OPS capabilities and to create the checkpoint of the future:

i. AIT

Overview: AIT systems use millimeter wave technology to detect undivested items on travelers. This OPS technology closes the security gap left by EMD by detecting both metallic and non-metallic items (such as explosives), and increases detection capability of metallic and nonmetallic threats, such as explosives.

Figure A27: AIT

The goal of the AIT program is to enhance the traveler experience further and to improve security by achieving a higher detection and lower false-alarm system with a gender-neutral algorithm. AIT has five primary planned milestones between FY 2024 and FY 2028, resource dependent:

- Post-implementation Review (FY 2024);
- Enhanced algorithm and wideband retrofit of current fleet (FY 2026);
- Next-generation OPS technology development (FY 2024);
- Next-generation OPS technology testing (FY 2026); and
- Integrate the low-Pfa algorithm for AIT to extend the effective lifespan of the current OPS TSE; and test and deploy Gender-Neutral Screening (FY 2022 budget), with funding dedicated to achieving better detection with very low Pfa (while maintaining Gender-Neutral Screening) in the FY 2024 budget.

Currently, the AIT fleet includes ProVision Automatic Target Detection (AIT-1) units and ProVision 2 (AIT-2) units. Although new requirements, including algorithm improvements and

enhanced pixel imagery, have exceeded the technical limitations of AIT system hardware, it will remain a key component of passenger screening, and is undergoing efforts to extend its life, including High Definition (HD)-AIT upgrade kits that enhance the current fleet.

Future State: TSA continues exploring the ability to conduct risk-based screening by changing detection algorithms dynamically to match the vetting category of the passenger being screened. TSA also is finalizing a wideband algorithm integration to improve image processing and to address a variety of threats. For example, TSA is testing an AIT universal Windows 10 operating system that will allow for open architecture while being platform-independent and for third-party participation in algorithm and other development. This should allow for faster and better options for improving AITs. Furthermore, the universal aspect will allow the software to support either AIT 1 or AIT 2, streamlining implementation.

TSA is conducting activities to connect these AIT units to a secure network. Connectivity will provide for automated metrics collection and eventually will allow centrally controlled configuration. This configuration will provide increased data accuracy and availability, reduced manual effort, and faster and less costly deployment of software configuration changes.

TSA and the DHS Science and Technology Directorate (S&T) are exploring algorithm integration and wideband development to advance the detection capabilities of current and future AIT systems. The next generation of passenger screening technology will offer enhanced image resolution by using a wider frequency bandwidth that supports more advanced algorithms for automated threat recognition and detection. Other R&D initiatives include:

- Retrofitting AIT units to enhance detection performance: After completing the testing phase, TSA is evaluating retrofitting the existing AIT fleet with government-owned enhanced algorithms that increase detection capability, lower false alarm rates, reduce the need for pat-downs, and enable gender-neutral screening. TSA also is exploring HD-AIT, an ongoing S&T National Labs project to realize next-generation AIT capabilities and to improve millimeter technology;
- Utilizing the open architecture principles of the universal Windows 10 software to leverage use of updated algorithms and improved graphical user interfaces on the current fleet without hardware or retrofit modifications;
- Integrating DICOS standardized data formats and OPSL standardized interfaces to enable more advanced functionality long-term, regardless of vendor. Functionality would include the ability to support multiple algorithms to improve detection performance, standardization of operator interfaces through the Common Workstation, and implementation of risk-based screening concepts;
- Establishing and characterizing a post implementation review methodology; and
- Exploring next-generation alternatives: Detection-at-range and small-size, flat-panel AIT capabilities have the potential use for primary screening, secondary screening, and insider threat detection. These capabilities will increase throughput and detection, will reduce false alarms and the contact rate between TSOs and passengers, and will improve the overall passenger experience.

Figure A28: AIT Funding Profile

AIT – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
AIT (O&S)	$38.5	$38.7	$38.7	$38.7	$38.7	$193.3
On-Person Detection/Next Gen AIT (R&D)	$5.0	$5.0	$5.0	$5.0	$5.0	$25.0
Total AIT	**$43.5**	**$43.7**	**$43.7**	**$43.7**	**$43.7**	**$218.3**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

ii. PSP Legacy EMD

Overview: EMDs detect potentially dangerous metallic threats and promote high passenger-throughput capabilities, allowing for rapid inspection of passengers in transit while maintaining compliance with strict standard 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. 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. PSP-Legacy is developing a DHS Strategic Sourcing Vehicle to procure additional Enhanced Metal Detectors to supplement Safety Stock. There are 1,402 EMDs in use (as of December 2022).

Future State: The systems within the legacy program will continue to provide primary and secondary screening capabilities for the checkpoint while new technologies are being developed to detect ever-evolving threats better. TSA will explore the possibility of procuring new AIT units in support of airport growth and expansion, within base budget and funding priorities.

Figure A30: PSP Legacy EMD Funding Profile

EMD – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
PSP Legacy WTMD	$3.3	$3.4	$3.4	$3.4	$3.5	$17.0
Total PSP Legacy EMD	**$3.3**	**$3.4**	**$3.4**	**$3.4**	**$3.5**	**$17.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

Future of the OPS Capability: The future state of the OPS capability focuses on detecting more threats with fewer false alarms, moving people through the checkpoint seamlessly, displaying information consistently across checkpoint technologies, and increasing secure network connectivity. TSA prioritizes investments in the following OPS R&D efforts:

- **Walk-Through Metal Detectors (WTMD:** OPS will conduct R&D for metallic and non-metallic walk-through or WTMD Alternative screening solutions. Small airports

across the country currently only have WTMD units and do not have an AIT unit. The Security Vulnerability Management Process and the risk group have identified this gap in the detection of non-metallic threats at the checkpoint as a risk. TSA's Requirements and Capabilities Analysis (RCA) and Acquisition Program Management will work together to evaluate potential alternatives to WTMD that provide both metallic and non-metallic screening for those small airports, screening of airline workers, and application of PreCheck® screening. As part of the Next-Generation OPS Program, OPS will be funding a Business Associate Agreement to identify other potential alternatives to the WTMD and demonstrate those systems in a lab environment that offer non-metallic screening with high throughput and a reduced footprint;

- **Open Architecture (OA)**: OPS will also play a critical role in moving towards an OA environment that frees TSA from proprietary systems from single vendors. Incremental demonstrations that showcase plug and play solutions in this environment will allow TSA to rapidly decrease the time it takes to deliver solutions to the field in the future. It is important to note that OPS is one of many participants playing key roles in validating and supporting the transition that could lead to a full integrated risk-based checkpoint, where data flows from start to finish with a specific passenger; and
- **Training Systems:** One of TSA's biggest challenges moving forward is the limited data set for training algorithms that will be required for future OPS systems. These include systems such as in-motion systems, shoe scanner solutions, and future algorithms. OPS will establish a synthetic data repository that aims to supplement a more cost efficient and reduce the labor-intensive process of clearing test passengers to gather data sets. With this repository, TSA will be able to provide these image sets to 3rd party vendors and encourage a new market of algorithm developers to provide TSA with new ATRs in an open architecture environment.

TSA envisions passengers advancing through the checkpoint seamlessly while achieving unparalleled security effectiveness using next-generation screening solutions.

4. Checked Baggage

Checked Baggage Capability Overview: TSA is congressionally mandated and responsible for the security screening of 100 percent of checked baggage. Checked baggage includes property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during the flight. As threats to our mission space continue to evolve, so must TSA's technology and mitigation strategies to ensure mission success. If an adversary is able to exploit security gaps in the global security infrastructure, the potential for harm to the traveling public increases exponentially, as gaps could be exploited in any airport nationwide and globally. The Checked Baggage capability manager (CM) mitigates evolving threats and capability gaps present in the checked baggage environment. The Checked Baggage CM Team, and other stakeholders both internal and external to TSA, are dedicated to guide the maturation of the Checked Baggage Capability across the TSA Enterprise. The primary objective for the team is to develop, acquire, and implement dynamic material and nonmaterial modular capabilities that will enhance TSA's ability to improve aviation security and the experience of the TSOs using Checked Baggage technology and capabilities.

Many ongoing and new efforts are occurring within checked baggage technology. TSA has successfully demonstrated the use of Checkpoint CTs to be used for both Carry-On and Checked Baggage at low volume airports and continues to develop this effort. TSA is exploring a developmental software to support the monitoring of screener performance, the measurement of operator performance, and the assessment of operator training effectiveness. TSA is also pursuing the advancement of threat detection algorithms on new and existing equipment to improve TSA's ability to detect a wider range of threats while decreasing the probability of false alarms. Newly developed algorithms are currently undergoing field test while R&D begins to characterize the next generation detection requirements. TSA is also exploring the abilities of smarter Baggage Handling Systems (BHS). Desired capabilities include routing passengers' baggage according to risk level and remote image recall. Furthermore, and in conjunction with the U.S. Customs and Border Protection (CBP) and the DHS Office of Science and Technology (S&T), the Checked Baggage CM is exploring a series of proof of concepts that will help determine the feasibility of screening baggage images remotely to eliminate TSA's need to rescreen baggage from abroad under the One Stop Security (OSS) initiative. TSA is also pursuing other technological solutions that decrease the need for opening bags.

Figure A31: Checked Baggage Capability Funding Profile

Checked Baggage FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Screening Technology Maintenance	$269.8	$270.3	$270.3	$270.3	$270.3	$1,351.0
Screening Technology Maintenance - Non Investment	$1.0	$1.0	$1.0	$1.0	$1.0	$5.0
Subtotal O&S	**$270.8**	**$271.3**	**$271.3**	**$271.3**	**$271.3**	**$1,356.0**
Checked Baggage - Electronic Baggage Screening Program (EBSP) - Investment (Discretionary Funding)	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0
Aviation Security Capital Fund (ASCF) - Electronic Baggage Screening Program (EBSP) - Investment (Mandatory Funding)	$250.0	$250.0	$250.0	$250.0	$250.0	$1,250.0
Subtotal PC&I	**$250.0**	**$250.0**	**$250.0**	**$250.0**	**$250.0**	**$1,250.0**
Total Checked Baggage Capability	**$520.8**	**$521.3**	**$521.3**	**$521.3**	**$521.3**	**$2,606.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

i. EBSP

Overview: The Aviation and Transportation Security Act of 2001 mandates that 100 percent of aviation checked baggage be screened by electronic or other approved means. To meet the mandate continually, the Checked Baggage Technology Division manages the EBSP. The EBSP is responsible for various mixed lifecycle acquisition activities, including the purchase and installation of security technologies at airports, upgrading fielded

Figure A32: EDS

technologies, and entering into other transaction agreements with airports. EBSP conducts these activities to test, procure, deploy, integrate, upgrade, and maintain technology to screen checked baggage for concealed explosives, focusing on the development and deployment of enhanced detection capabilities to improve security effectiveness and to support operational need.

The Checked Baggage fleet consists of approximately 1,665 Explosive Detection Systems (EDS). Contained within these EDS are 225 Smiths Detection CTX 9000 and CTX 9400 systems, as well as 14 CTX 5500 systems which are all End of Life (EOL) and in the process of being recapitalized. These systems are used as a primary screening device and consist of both Type 1 (in-line) and Type 2 (stand-alone) systems that are deployed based on baggage volume. The EBSP fleet also has 2,439 ETD devices used predominately as an AR tool, but also are used for primary screening where baggage volume or infrastructure limitations do not support EDS operations.

EBSP works to streamline the acquisition process to help provide greater predictability to manufacturers wherever possible. This is done through competing EDS unit purchases for recapitalizations and new in lines wherever feasible allowing manufacturers to plan years in advance of the TSA's need, hosting Industry Days for new opportunities, and reporting competitive work through the Acquisition Planning Forecast System.

Future State: EDSs are a robust and mature technology with an enduring useful life and are designed with inherent capability expansion. EBSP is a sustainment program that manages the EDS useful life and technical obsolescence closely with an emphasis on improving the fleet's performance through targeted capability enhancements vice full-scale system replacement. This approach allows TSA to procure technologies and to upgrade existing systems with enhanced capabilities at a significantly lower cost, instead of replacing entire systems. TSA continues to develop the necessary technical advances under EBSP to address threat vulnerabilities across hundreds of federalized airports. Planned technology enhancements include the following:

- Development and deployment of EDS algorithms to advance detection capabilities through the expansion of the systems' threat detection library, reducing the amount of detectable threat mass, reducing the false-alarm rate, and focusing detection on adversarial threat preference;
- Defining cybersecurity requirements for future compliance;
- Image format standardization; and
- Recapitalization of technically obsolete EDS machines.

With a substantial infrastructure required to support Checked Baggage operations beyond the EDS and ETDs, TSA is developing a capability roadmap and aiming to implement technology and infrastructure improvements to support the future vision of Checked Baggage.

Future of the Checked Baggage Capability: Qualification of new capabilities under the next investment from the start of testing through addition to the Qualified Products List is anticipated to take at least three years; however, changes to the test methodology from the previous

qualification windows under EBSP are anticipated to lower incidences of failure by working hand-in-hand with manufacturers during the early stages of testing.

The future state of this Capability is to enable secure and remote data transmission to derive meaningful and data-driven insights in NRT as well as operationalize threat assessments. Checked baggage EDS machines will be connected and move into cyber compliance. The "Enable" functional area refers to efforts that facilitate future enhancements of existing and emerging technology. The Capability future state is to leverage an open architecture concept and move towards enhanced capabilities around Common Workstation and remote data transmission. This would increase TSO deployment flexibility, optimize TSO training, and enable data transmission between international partners to decrease duplicative baggage screening.

The future outlook of Checked Baggage is divided into three functional areas/capabilities: Detect, Connect, and Enable.

- **Detect:** The "Detect" functional area refers to employing technology to determine if threats are present in checked baggage, ensuring the highest probability of detection with the lowest Pfa, while maintaining baggage throughput.
- **Connect:** The "Connect" functional area refers to leveraging information technology (IT) systems to allow for NRT data capture. As such, NRT data capture can enable and empower data-driven decision making at TSA to inform and optimize the allocation of airport resources. The future state of this capability is to enable secure and remote data transmission to derive meaningful and data-driven insights in NRT, as well as to operationalize threat assessments. Checked baggage EDS machines will be connected and will move into cyber compliance.
- **Enable:** The "Enable" functional area refers to efforts that facilitate future enhancements of existing and emerging technology. The capability future state is to leverage an open architecture concept and to move toward enhanced capabilities around Common Workstation and remote data transmission. This would increase TSO deployment flexibility and interoperability pertaining to Checked Baggage technologies, would optimize TSO training that could be applied to Common Workstation, and would enable data transmission between international partners to decrease duplicative baggage screening.

To advance long term future-state capabilities specific to the TSA mission and maintain adequate security for a growing traveling population, TSA must expand access to R&D investments through interagency and industry partnerships, not just requests for additional funding. For Checked Baggage screening, TSA is pursuing R&D with potential to implement enhanced threat detection algorithms on new and existing TSE to improve TSA's ability to detect wider range of threats while decreasing the probability of false alarms.

In addition to enhanced algorithms, TSA is pursuing additional capabilities such as the use of artificial intelligence and machine learning. These efforts will involve significant up-front human and financial resource allocation. Furthermore, to improve the performance and capability of existing Checked Baggage screening systems, TSA will continue to seek

enhancements to their EDS. Also, TSA seeks to improve AR technology and integration of this technology into the baggage handling system.

TSA is exploring new detection capabilities such as X-ray diffraction and Differential Phase Contrast to improve detection of homemade explosives across EDS platforms and decrease the probability of false alarms. Overall, TSA will leverage R&D investments for checked baggage screening in order to expedite the development of state-of-the-art and automated high-speed, high-performance checked baggage EDS with improved material discrimination/identification, improved throughput, and reduced operations and maintenance costs for TSA acquisition.

For some airports that lack EDS, TSA can provide CTs as part of the dual-use CT. By utilizing deployed checkpoint CT, TSA will no longer depend on physical search utilizing ETD screening for Checked Baggage.

5. Multimodal and Public Area Capabilities (MPAC)

Overview: MPAC provides security technology recommendations and solutions for air cargo, public transportation areas, and critical infrastructure (such as pipelines). Various multimodal capabilities align to TSA's mission and focus area. Surface Security Technology (SST) evaluates advanced technologies and facilitates industry awareness to address identified capability gaps in surface transportation security. Airport Infrastructure Protection (AIP) identifies capability gaps to provide airports with robust infrastructure protection to improve airport security and situational awareness. The Air Cargo Security Program collaborates with industry to develop requirements and to qualify technologies to address identified capability gaps in air cargo screening security.

Figure A33: MPAC Funding Profile

MPAC – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Surface Programs - Ops	$7.9	$7.9	$7.9	$7.9	$7.9	$39.5
Air Cargo - Ops	$10.9	$10.9	$10.9	$11.0	$11.0	$54.7
Mission Support - Non Investment	$3.3	$3.3	$3.3	$3.4	$3.4	$16.7
Total MPAC	**$22.1**	**$22.1**	**$22.1**	**$22.3**	**$22.3**	**$110.9**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

i. SST

Overview: TSA has extensive experience working with transportation operators and industry manufacturers to implement, assess, and refine late-stage high technology-readiness level mature security technologies. MPAC Surface was established in 2004, after the Madrid and London attacks. The program has evolved and grown, leading and promoting innovation within surface transport venues for almost 16 years.

SST test beds provide a critical capability for evaluating the operational performance and suitability of candidate technologies in surface transportation environments. TSA has active test bed agreements with 19 surface transportation entities, and MPAC manages installation, evaluation, and testing in more than 26 sites across the United States and throughout all surface transportation modes.

MPAC surface mission areas are directed by public law, executive orders (EO), Presidential Policy Directives (PPD), and national/supporting plans. In addition, the program supports the requirements of the DHS National Infrastructure Protection Plan established in accordance with Homeland Security Presidential Directive (HSPD)-7 and the requirements of PPD-21. Specifically:

- 6 United States Code, Chapter 4: Transportation Security;
- The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) Titles XIII and XV;
- EO 13416: Strengthening Surface Transportation Security; and,
- The FAA (Federal Aviation Authority) Reauthorization Act of 2018 (P.L. 115-254) Subtitle G, Sec. 1968.

Test bed evaluations offer system partners extended access to and use of promising technologies preceding any procurement decisions. Evaluated technologies then are placed in the annual SST Catalog. Representation in the SST Catalog does not indicate endorsement for a technology's capabilities or performance, but rather provides an unbiased representation of the results of the complete scope of standardized security technology assessments and industry engagement efforts.

Future State: Current and upcoming TSA initiatives include: handheld/standoff explosive detection testing; lab and field testing of next-generation detection-at-range passenger, baggage, and vehicle screening systems; rail undercarriage screening system pilots; ongoing evaluation of emerging intrusion detection technologies; and chemical detection software integration.

Figure A34: Detection-at- Range

Figure A35: Undercarriage Screening

Figure A36: Standoff Optical Trace Detection

TSA SST will continue to support operational test beds for different modes of transportation (mass transit, highway motor carrier, pipeline, freight rail, and maritime), public areas, and

critical infrastructure protection (including airport perimeters) security technology projects to address the increasing threat demonstrated from attacks worldwide. Due to the evolving threat of attacks at different surface venues, SST's test beds will continue to**:**

- Provide a critical capability for evaluating the operational performance and suitability of candidate technologies in surface transportation environments;
- Offer system partners extended access to and use of promising technologies prior to making procurement decisions; and
- Afford transportation systems and venues the opportunity to provide direct feedback to TSA and to technology vendors so that product configurations and concepts of operations are optimized for use in surface transportation environments.

Figure A37: SST Funding Profile

SST – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Surface Programs - Ops	$7.9	$7.9	$7.9	$7.9	$7.9	$39.5
Total SST	**$7.9**	**$7.9**	**$7.9**	**$7.9**	**$7.9**	**$39.5**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

ii. Air Cargo Security Technology Program

Overview: The Air Cargo Management Systems (ACMS) Branch engages with TSA and industry stakeholders to develop IT and data solutions in support of the implementation of TSA's Air Cargo Program. ACMS accomplishes this goal by managing a host of IT systems used as tools and resources by both internal and external entities. The policy requirements and priorities linked to security programs are supported and implemented via the on-going development of these systems. Currently, ACMS provides access to IT systems that facilitate TSA's efforts to ensure the security of cargo transported on passenger aircraft. These systems are used by over 35,000 industry users; vet approximately 7.3 million shippers and 450,000 air cargo workers; and support regulation of nearly 4,000 Indirect Air Carriers (IACs).

The IT systems within the portfolio, three major and two minor applications, include the following: the Indirect Air Carrier Management System (IACMS), the Freight Assessment System (FAS), and the Known Shipper Management System (KSMS), the Certified Cargo Screening Facility Tool (CCSFT), and the Security Threat Assessment Tool (STAT). These systems work to confirm the identity and business legitimacy to assess the risk of companies shipping goods on passenger aircraft (KSMS); vet individuals in security sensitive positions to reduce the risk from insider threats (IACMS, STAT); ensure entities transporting and screening air cargo employ appropriate security procedures (IACMS); provide historical cargo reporting data (FAS); and facilitate air cargo data sharing across TSA (all systems).

Future State: MPAC's Air Cargo Branch recently completed a landscape study of Air Cargo Screening Technology List (ACSTL)[18] screening technology. This study illuminated that approximately 1,600 screening devices (i.e., visual image X-Rays, ETD devices, EMD devices, and EDS, which are listed on the ACSTL) are currently being used by about 170 private entities at about 750 domestic sites. ACSTL listed technologies influence screening technology used at many high-risk Last Points of Departure bound for the U.S. venues. Furthermore, many U.S. partners cannot afford a proper test and evaluation program, so they rely on the ACSTL to identify screening technologies for use.

TSA is shortening the ACSTL by identifying less capable and obsolete embodiments of screening technology and grandfathering their use. Fifteen models of EDS were removed from the ACSTL at the end of 2022.

In terms of ubiquity of the number of screening devices in use domestically in air cargo, ETDs are the most numerous, numbering at about 1,100 ETD devices. All of the five ACSTL ETD models are set to be removed from the ACSTL by the end of FY 2024, if not sooner. Currently, there are only two ETD models undergoing field testing – Smiths Detection IONSCAN 600 and Rapiscan Itemiser 5X. Two additional ETD models – Bruker DE-tector flex and Leidos QS-B220 – are undergoing laboratory testing. If successful, field testing will follow. TSA is optimistic that at least one of these ETD models will be available for purchase before the ACSTL grandfather expiration date.

For imaging-based air cargo screening technologies, dual-view X-rays comprise a majority of ACSTL listed devices, which are available for private purchase. Though there are far fewer X-rays (i.e., approximately 500 devices) in use domestically, X-rays have considerably higher throughput relative to ETDs, and in turn, screen a larger proportion of air cargo. Large aperture X-ray, capable of screening homogeneous pallets, are the most frequently used version of X-ray. Improvements in X-ray image quality, especially penetration performance as the presence of opaque and therefore uninspectable regions most negatively impact screening operations, drive manufacturer development and ultimately expansion of the ACSTL with the addition of high-performance models.

The International Civil Aviation Organization (ICAO) mandate on international all-cargo screening ushered in the adoption of high-speed EDS technology. eCommerce and other fast parcel operations can benefit from the high throughput screening offered by this technology despite the high capital investments costs associated with technology and automation. An additional EDS – Smiths Detection HI-SCAN 10080 XCT – is preparing for field testing. If successful, it will provide competition in the marketplace.

Regulated parties and manufacturers have expressed interest in small aperture EDS (as developed for the Checkpoint Property Screening System program), which have applicability for

[18] To meet its air cargo regulatory responsibilities, TSA qualifies screening equipment and publishes a list of authorized systems. Regulated Parties, which include airlines, TSA Certified Cargo Screening Facilities, and their authorized representatives may only use technology screening systems listed on the ACSTL under TSA Security Programs. All systems listed on the ACSTL must comply with the TSA minimum requirements based on the relevant technology type.

break-bulk and counter-to-counter cargo screening applications. TSA has developed and issued requirements updates to facilitate future inclusion on the ACSTL.

TSA's focus remains facilitating incremental improvements to existing technology for enhancing threat detection, cost, suitability, and sustainment. By leading the TSA Air Cargo Security Technology Working Group, both TSA and DHS S&T annually gather input from air cargo transportation stakeholders for the development of technology capability gaps to guide government spend plans and resources.

Figure A38: Air Cargo Security Technology Program Funding Profile

Air Cargo – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Air Cargo - Ops	$10.9	$10.9	$10.9	$11.0	$11.0	$54.7
Total Air Cargo Security Technology Program	**$10.9**	**$10.9**	**$10.9**	**$11.0**	**$11.0**	**$54.7**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

iii. AIP

Overview: AIP provides airports with robust infrastructure protection to maintain airport security and situational awareness by using security technology to support identification, management, and mitigation of terrorist and other aviation security threats. AIP uses a sophisticated combination of cameras and analytics sensors to significantly increase overall operational and situational awareness, including detection of intrusions and other unauthorized events and potential threats.

The FY 2018 DHS Appropriations Act allocated up to $10 million for TSA to develop "a multi-year plan to analyze and test perimeter intrusion detection and deterrence technologies in partnership with airports." Through risk-based methodologies, TSA selected one CAT X and one CAT I airport through Other Transactional Agreements (OTA) to test and analyze perimeter security technologies. This project will help highlight the vulnerabilities at the perimeter of airports and secure additional funding for further perimeter protection projects. TSA will conduct two years of data collection and develop a final report based on lessons learned, recommendations for the industry on enhancing perimeter intrusion technologies, and provide insights on operational benefits to installing such technologies at the perimeter of critical infrastructure.

OTAs are an important tool to meet mission needs with local airport authorities. In 2018, AIP funding for closed-circuit television (CCTV) OTAs was eliminated, removing TSA's ability to provide CCTV security enhancements for airport public areas.

Future State: As of December 2022, the CAT X Perimeter Intrusion Detection airport had completed 95 percent of the installation phase of the project and the project is slated for completion during FY 2023, second quarter. Once installation is complete, TSA will collect data

for up to two years to help highlight the vulnerabilities at the airport perimeter and provide the industry with lessons learned. Once these projects are completed, resources will be needed to continue these test beds, including needed refresh of the technologies as the marketplace advances.

TSA should continue to expand partnerships and assess next generation technologies to understand their potential to address the critical capability gaps in the public areas of airports. One area that TSA has seen a significant interest in is the exit lanes at airports and installing automated exit lane technologies. Airports have recognized the operational efficiencies, cost benefits, and security capabilities of eliminating the human element from installing automated exit lanes and are searching for an independent evaluation of the effectiveness of marketplace technologies.

iv. Automated Exit Lanes

Overview: Approximately 25 percent of federalized airports have automated exit lanes as of December 2022; most airport exit lanes are manned by TSOs during peak airport hours. The FAA Reauthorization Act authorized $15 million per year from FY 2019 to FY 2021 for TSA to test exit lane technologies, but no funds were appropriated. TSA conducted a limited assessment of exit lane technologies to analyze automated technology, to collect feedback on airports' use of the technology, and to identify variables to consider when assessing the financial feasibility of installing automated exit lanes. In September 2020, TSA developed a congressionally mandated report to highlight the cost benefits of installing automated exit lane technologies.

TSA partnered with eight airports (MDW, MEM, LAS, MIA, DTW, SJC, BWI, and DCA) to conduct an internal study of Exit Lanes. In November 2022, TSA performed several site visits to collect data on the airports' current exit lane capabilities and potential areas of improvement and that would meet their requirements. TSA successfully collected data on five of the eight airports through site visits and leveraged previously obtained data from the other three airports to generate the finding of the Exit Lanes Internal Study. TSA will use this data to inform the industry on the operational and security benefits, cost benefit analysis, and lessons learned.

Future State: TSA has made significant progress in understanding the capability and feasibility of exit lane technology replacing or augmenting the human exit lane security model.

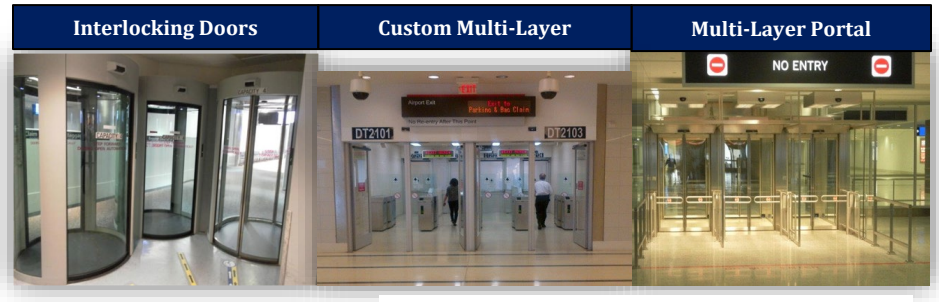


Figure A39: Automated Exit Lanes

TSA continues to leverage its existing relationships with industry technical experts and vendors to further analyze the benefits of installing exit lane technologies to safeguard the traveling public. To advance TSA's priorities and mission progress AIP requires continual and additional

support to visit additional sites and collect operational data on automated exit lanes installed to test further and to recommend technologies to airport stakeholders. Congressional and industry stakeholders have expressed interest in assessing whether the use of technology can improve exit lane security while decreasing long-term personnel costs. TSA sees the benefit of cost savings in TSO labor if technology is sufficient, although funding remains a challenge. TSA's belief that technology has matured to where demand for equal or better security at a lower cost can be met was confirmed by the results of the study. The study suggests that TSA can achieve substantial lifecycle cost savings with exit lane technology.

v. Public Areas

Overview: Public areas are critical aspects of freight rail, mass transit, highway motor carrier, pipeline, airport infrastructure, and maritime modes of transportation. In public areas, traditional security screening procedures that require divestment of articles from travelers and an intrusive and slow search process are unrealistic. To address the complex security needs of mass transit stakeholders, TSA assesses the value of video analytics and detection-at-range technologies as part of a sophisticated layered approach for adequate protection, while ensuring freedom of movement for the travelling public.

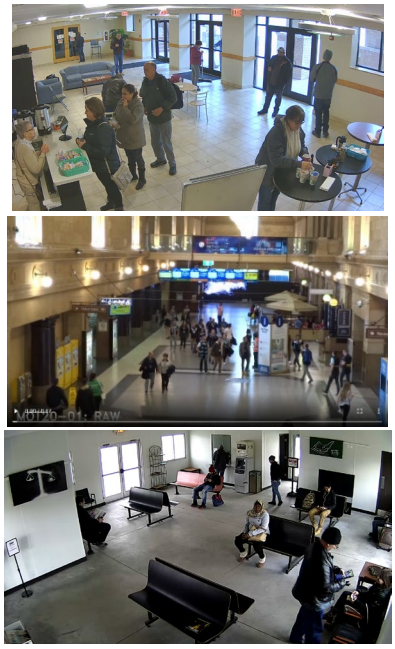


Figure A40: Airport Public Areas

Future State: TSA is continuing to work with detection-at-range technology vendors to test new iterations of their products and to provide operator feedback for improving product capabilities. In addition, TSA is exploring how emerging screening and surveillance technologies can be leveraged in a risk-based approach to securing crowded public areas. These systems enable effective screening of the traveling population "on the move" and provide real-time information about a traveler's potential threat to the local population and environment, enabling well-informed decisions about initiating an escalation of security protocols. These systems will continue to enhance screening by layering technologies using combinations of sensors and analytics systems to increase overall operational awareness significantly, and to detect anomalies and other suspicious behavior.

vi. Critical Infrastructure

Overview: 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, across any federal, state, regional, territorial, or local jurisdiction. TSA supports 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.

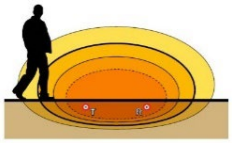


Figure A41: Buried Line Sensors

Figure A42: Laser Scanner/ Lidar Sensors

Future State: TSA will continue to identify, test, and evaluate layered technologies for sophisticated infrastructure protection using combinations of sensors and analytics systems to increase overall operational awareness and to detect intrusions and other unauthorized events.

Figure A43: IP Cameras

vii. Chemical/Biological

Overview: TSA leverages technical and analytical support from National Laboratories and collaborates with DHS S&T and the Countering Weapons of Mass Destruction Office in chemical and biological protection, particularly in surface transportation venues. The purpose of the support is to provide prevention, timely detection/identification, situational awareness, and efficient mitigation and response to chemical and biological threats. TSA collaborates with DHS S&T's Chemical/Biological Defense Division to evaluate reliable and robust chemical sensing technologies to enhance multimodal transportation security. Transportation systems use chemical detection for:

- Layered defense for full system protection;
- Automated alarms in tandem with other sensors;
- Confident threat determination with minimal false alarms;
- Force multiplier with minimal impact to operations (autonomous systems); and
- Modular and robust solution that can be extended to other sites/venues.

TSA participates in and follows S&T biodefense activities but does not have sufficient resources to participate in activities beyond representing TSA needs, gaps, and requirements. Due to mass transit venues being more concerned with chemical and flammables threats, introduction of bio sensing into standing test beds is limited. Mass transit, passenger rail, and airport authorities, however, do collaborate extensively with and participate in the DHS Office of Health Affairs biodefense programs and pilot testing.

Future State: Continued and future test-bed activities include:

Figure A44: Chemical Detectors

- Evaluate standoff chemical vapor detectors where the objectives are to: evaluate the performance of current systems, characterize backgrounds, and perform modeling and simulation as well as algorithm development.
- Leverage previous DHS S&T Chemical/Biological Defense Division investments in detector development and operational test beds to bridge the gap between chemical detection security requirements for mass transit and technology manufacturers products.
- Support development of algorithms to prevent, detect, and alert authorities more accurately to chemical spills in mass transit environments.
- Use installed initial chemical detection capabilities at mass transit venues to identify technology gaps and to socialize concept of chemical detection.

Future of MPAC: TSA intends to continue enhanced threat detection for multimodal screening systems by continuing to invest in primary and secondary screening across the multimodal transportation infrastructure. TSA's goal is to increase detection capability for known threats, to increase 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).

TSA evaluations and investments drive multimodal technology vendors to develop and enhance their equipment and systems by facilitating operational improvements to technologies that increase multimodal security.

6. Counter-Unmanned Aerial Systems (C-UAS)

Overview: 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 has long standing authorities and responsibilities to conduct testing, evaluation, and assessments of technology supporting TSA's mission responsibilities established by public law, EOs, National Security Memorandums (NSMs), and national/supporting plans. The TSA C-UAS Test Bed Program meets additional requirements in the Preventing Emerging Threats Act of 2018, to "conduct research, testing, training on, and evaluation of any equipment, including

any electronic equipment, to determine its capability and utility prior to the use of any such technology" for any authorized C-UAS action.

The Preventing Emerging Threats Act of 2018[19] includes C-UAS authorities for DHS and DOJ that may or may not expire. If these authorities expire, the scope of the technologies TSA would be authorized to test would be significantly impacted. TSA would have the ability to maintain the testbeds under other authority, but the range of technologies TSA would be authorized to test would be much more limited.

TSA established the C-UAS Test Bed Program and is currently assessing technology effectiveness and suitability in operational airport environments. The C-UAS test beds are ongoing and scalable, continuously testing equipment to keep up with the rapidly developing capability of the adversary, advances in UAS capability and technology, and the ever-evolving counter-UAS technology marketplace. Technologies are being introduced through incrementally complex phases, each building on lessons learned during our testing process. TSA shares in-progress data summaries of technology testing results, best practices, and lessons learned with appropriate interagency stakeholders so that they also may benefit from the information gleaned at the test beds.

TSA is working closely and sharing information with its interagency partners, including the FAA and S&T, to establish test beds for UAS detect, target, intercept (DTI) technology at MIA and LAX. Additional airports and high value surface venues are a high-priority item for DHS and Congress, and test beds will be established as additional resources are provided.

Future State: The TSA C-UAS program must remain ahead of the adversary by understanding UAS threats, vulnerabilities, and potential countermeasure systems clearly. The number of encounters with UAS around airports and with civil aircraft has increased due to UAS proliferation

TSA completed its first flight test event at MIA, flying over 100 sorties using seven UAS models against six UAS DTI systems, and is analyzing results to be shared with appropriate stakeholders. TSA installed the first DTI technology at LAX and began system configuration to the airport's unique environment before collecting data. TSA is coordinating with LAX and other stakeholders to continue the establishment of the test bed and plans to begin technology testing in FY 2023.

The capabilities of UAS continue to advance rapidly. With the advent of autonomous operation and 5G mobile network, the UAS fly longer, faster, and with heavier payloads, and they will continue to pose an increased risk to the aviation domain. With the recent negative impacts to commercial aviation and the lack of federal capabilities, many airport authorities independently acquire their own UAS detection and mitigation systems. This potentially poses more danger at airports and results in operational and procurement inefficiencies with the deployment of disparate and uncoordinated systems.

[19] S.2836 - 115th Congress (2017-2018): Preventing Emerging Threats Act of 2018 | Congress.gov | Library of Congress: https://www.congress.gov/bill/115th-congress/senate-bill/2836/text

To address these issues, 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 with information gleaned from the test beds 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 program will also incorporate UAS testing at surface test bed locations if funding is available.

Information gathered from testing these systems at C-UAS test beds will have the ability to benefit thousands of critical infrastructure sites, as TSA will share testing results, best practices, and lessons learned with state, local, tribal, territorial, local law enforcement, the airport authority, and with 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.

Figure A45: C-UAS Funding Profile

C-UAS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Aviation Screening Operations	$6.2	$6.2	$6.2	$6.2	$6.2	$31.0
Mission Support	$1.0	$0.8	$0.8	$0.8	$0.8	$4.2
Other Operations and Enforcement	$4.1	$4.5	$4.6	$4.7	$4.7	$22.6
Total	**$11.3**	**$11.5**	**$11.6**	**$11.7**	**$11.7**	**$57.8**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

7. National Explosives Detection Canine Team Program (NEDCTP)

Overview: The NEDCTP is a congressionally mandated program[20] that allocates Explosives Detection Canine (EDC) teams to the aviation, rail, maritime, and mass transit transportation systems. TSA has used two types of canine teams: Law Enforcement Officer (LEO)-led canine teams and TSA-led canine teams. Of the 1,097 teams, 422 are TSA-led Passenger Screening Canine teams, with the remaining 675 teams typically being LEO-led. Of those 675 LEO-led teams, 156 were focused in the maritime, rail, and mass transit environments.

Canine teams remain an integral component of TSA's strategy against terrorist use of improvised explosives devices. Canines are a unique mode of explosives detection that has proven to be versatile, mobile, and effective in both detection and deterrence. TSA's EDC program began in 2002, when the FAA fully transitioned its canine program to TSA. TSA trains and deploys certified EDC teams to detect and deter the introduction of explosives devices into the aviation, mass transit, rail, maritime, and cargo security environments. Despite technological advances in

[20] Section 110, paragraph (e) (3) of the Aviation and Transportation Security Act (P.L. 107-71); the Homeland Security Act of 2002 (P.L. 107-296); and the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53).

analytical instruments, a well-trained and supported EDC is the most used and effective detector of explosives.

TSA has used EDC teams led by local LEOs, through partnerships with state and local law enforcement agencies (LEA). LEAs voluntarily participate in the program and sign interagency cooperative agreements with TSA. A LEO-led canine team consists of one EDC that is highly trained in scent detection tasks for explosives detection on stationary objects such as vehicles, bags, aircraft, buses, ferries, cargo, and warehouses, and one handler who is trained and experienced in interpreting the behaviors of the canine. Through partnerships with state and local LEAs, TSA has provided a canine for each handler, initial team training, sustained team training, annual certification, and an annual stipend to partially reimburse each participating LEA for operational costs for maintaining the canine teams. However, the FY 2024 President's Budget did not include that stipend for LEO reimbursement canine teams.

The size, scope, and complexity of canine operations has expanded as TSA received appropriations for additional canine teams. In 2007, TSA implemented TSA-led Cargo Proprietary EDC teams and transitioned to TSA-led Passenger Screening Canine teams in 2011.

A TSA-led canine team consists of one Passenger Screening Canine, that like an EDC is trained in scent detection tasks for explosives detection on stationary objects, as well as on moving passengers and their personal belongings, and one handler who is trained and experienced in interpreting the behaviors of the canine.

In 2018, TSA began the Third-Party Canine Cargo (3PK9-C) screening program, operating under a TSA security program. The program was congressionally mandated in the TSA Modernization Act, Section 1941, and TSA collaborated with air cargo industry to develop and implement the 3PK9-C program. The purpose of the 3PK9-C program is to mitigate the 100 percent of outbound international air cargo screening requirements mandated under the ICAO, which TSA adopted as a requirement. DHS S&T has designated the certified 3PK9-C canine teams as a screening technology under the DHS Safety Act. Within the aviation environment, TSA-led canine teams traditionally have focused their efforts at the checkpoint. LEO-led canine teams traditionally have focused their efforts in the public area and threat response throughout the transportation modalities.

TSA provides state and local law enforcement agencies with handler training courses and a certified EDC, annual onsite evaluations/certification, current threat explosive canine training aids, and state-of-the-art web-based applications for administrative documentation.

However, without a centralized authority to manage capability analysis and solutions, requirements development for the entire canine program, integration of detection capabilities, and assets alignment throughout the security environment, TSA experienced challenges developing and executing a holistic, long-term strategy for the canine program. As TSA had addressed similar organizational challenges for other security screening capabilities successfully, the Canine Capability Management Team was created in November 2020 to address these challenges. The Canine Capability Management Team oversees and aligns capability

development efforts and requirements for TSA's multiple canine program offices listed below, to include the 3PK9-C program.

Figure A46: NEDCTP

Future State: TSA will pursue integration of proven canine detection and deterrence capabilities throughout the entire aviation, mass transit, rail, maritime, and cargo transportation security environments. Accordingly, TSA will improve effectiveness of all canine teams performing in the aforementioned transportation domains through performance and development research, increased utilization and deterrence, improved communication, education, relationships, and accountability. TSA will build a collaborative, layered canine security plan to detect and deter explosive threats better from entering into the aviation, mass transit, rail, maritime, and cargo environments.

Figure A47: NEDCTP Funding Profile

NEDCTP – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
NEDCTP	$158.7	$166.7	$174.1	$178.9	$182.4	$860.8
Canines - K-9 System - Investment	$2.7	$2.7	$2.7	$2.7	$2.7	$13.5
Third Party Canine Program	$1.6	$1.8	$1.8	$1.8	$1.8	$8.8
Total Canines	**$163.0**	**$171.2**	**$178.6**	**$183.4**	**$186.9**	**$883.1**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

C. Enhanced and Secure IT Systems

1. Information Technology Infrastructure Program (ITIP)

Overview: The ITIP provides secure and reliable IT and communications products, services, and solutions, which support TSA in accomplishing its essential national security mission of protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. ITIP is comprised of 34 FISMA-approved systems that support the TSA IT Enterprise, mission-essential operations, and law enforcement.

ITIP provides support and sustainment of IT services to approximately 70,000 federal employees, contractors, and support personnel at more than 600 sites worldwide. It manages the 24x7x365 operations, maintenance, and service of the IT infrastructure to ensure uninterrupted operational availability of IT services that are required for all business and mission needs (including operations, engineering, end-user services, application development, information assurance, enterprise architecture, and mission support). ITIP executes an IT service delivery model that meets TSA's service level requirements in a consistent, timely, and effective manner while providing reliable, sustainable, and standards–based technology including:

- Technical support and enhancements of the IT capabilities required by TSA's domestic and international workforce;
- Design and implementation of TSA-directed system and infrastructure changes, integrating them into the operations & maintenance (O&M) support model;
- Promotion of cybersecurity support activities to implement any mitigation or remediation actions associated with security incidents, active threats/intrusions into TSA systems, or identified vulnerabilities to maintain the security and protection of the TSA IT environment in accordance with FISMA, National Institute of Standards and Technology, and Office of Management and Budget (OMB) and DHS directives, policies, and guidelines; and
- Project management, engineering, and deployment services to address special project installs, moves, adds, and changes for TSA Headquarters, field sites, and airports.

ITIP is pursuing migration of operational assets to cloud-based environments where possible. As of March 2022, 22 applications have been migrated successfully to the TSA Azure (TAZ) cloud infrastructure. TAZ is continuing the transformation of ITIP through the identification and support of refactoring, or re-writing, applications from on-premises to the cloud environment. TAZ gives ITIP the ability for developing, testing, building, and deploying applications for specific platforms, further creating efficiencies and reducing the physical footprint within TSA's IT enterprise.

Future State: Future investments will enable TSA to continue providing IT equipment and services across TSA. ITIP will continue prioritizing investment in the following five initiatives to advance the program closer to the desired future state:

- **Cybersecurity:** One critical area TSA is involved with is Zero Trust Architecture (ZTA). In accordance with the EO 14028 on Improving the Nation's Cybersecurity and OMB-issued memorandums, ITIP is working on implementation plans to achieve ZTA goals by end of FY 2024. ZTA holds a key tenet that no network is implicitly considered "trusted". All traffic, to include internal traffic, must be encrypted and authenticated as soon as practicable. ITIP will ensure TSA's migration to cloud technology adopts to the foundational tenant that no actor, system, network or service operating outside or within the security perimeter is trusted. Also, implementation plans will move TSA to an architecture that verifies anything and everything attempting to establish access. This migration is a paradigm shift in philosophy of how TSA secures its infrastructure, networks and data, from verify once at the perimeter to continual verification of each user, device, application, system, service and transaction.

  Additionally, as part of the IT Focus Priorities, ITIP will enhance and expand embedded security in all phases of the system development lifecycle to include post-deployment operations, maintenance and upgrades. ITIP's success and that of the entire TSA IT enterprise hinges on secure IT and data. Cybersecurity will be designed and built into all projects/acquisitions/services, continually monitored and upgraded throughout. ITIP also will expand partnerships to drive threat intelligence reporting and to increase awareness within the overall DHS environment. Among these emerging initiatives for increased

cybersecurity support, ITIP will continue the current cybersecurity efforts provided to more than 70 FISMA systems at TSA without interruption.

- **Cloud:** ITIP continues its advance to a cloud-based service model that is making delivery of critical IT services more agile, efficient, and cost-effective. ITIP is at the forefront of accelerating TSA's capability to expand cloud offerings, focusing on the transition of existing TSA applications to operate in the Federal Risk and Authorization Management Program authorized commercial cloud(s) using commercial design patterns and best practices. In FY 2022, ITIP partnered to transition an additional three business applications to TAZ from on-premises. This includes the Law Enforcement/Federal Air Marshals (LE/FAMS) and IT transition of TSA's Real-Time Analytic Platform for Incident Deterrence (RAPID) application. This was a significant and collaborative effort to refactor, re-platform and modernize TSA's RAPID application. The application was successfully transitioned from an on premise hosted solution using 2008-2014 technology to a hybrid cloud solution hosted in the TAZ system. RAPID is TSA's first business application to leverage Microsoft Azure Platform-as-a-Service (PaaS) offerings (e.g., Azure Search and Azure SQL) that utilize the latest cloud-based technology capabilities. The migration to TAZ currently provides the RAPID application higher availability, scalability and redundancy. The utilization of Azure PaaS cloud-based services ensures RAPID continues to leverage cutting-edge technology for search and database capabilities now and moving forward. The adoption of cloud solutions/services, such as integrations between the current on-premises enterprise to Infrastructure-as-a-Service (IaaS), PaaS and Software-as-a-Service (SaaS), transforms the enterprise from that of an asset-based organization to a service-based collaboration and cooperation IT delivery approach that will ensure mission success. These technologies will reduce costs and bring efficiencies into the way that IT services are delivered. The focus will shift to providing mission-essential IT services while significantly reducing requirements for hardware infrastructure recapitalization.
- **O&M:** Future O&M support for maintaining the enterprise services provided under ITIP is vital. These investments are critical to meeting TSA-required capabilities and include a vast array of IT professional services, hardware, software and network infrastructure that support TSA's ever-expanding and diverse technological environment. ITIP will maintain a high level of system availability and performance through maintaining/ upgrading software and hardware, improving system redundancy and upgrading networks. A standard annual refresh cycle provides TSA with a planned approach to addressing IT obsolescence. This ensures that hardware and software baselines meet end-user and application capability requirements and prevents security vulnerabilities associated with end-of-life assets. One of those efforts is the refresh of all Datacenter and field switches in the TSA infrastructure. These switches are critical components of the network and provide connectivity for all TSA operational computer systems and devices. Switches currently in use are end of life and, in some cases, beyond vendor support, so possible degradation and failures in common applications and systems may result if these switches are not replaced. Also, switches that are unable to be patched become security vulnerabilities for the agency. TSA requires a refresh of these switches to ensure the enterprise network infrastructure runs optimally and reduces security vulnerabilities and outages.

Another O&M effort will be the continued implementation of IPv6 throughout the IT environment. IPv6 is the next-generation Internet Protocol (IP), designed to replace version 4 (IPv4) that has been in use since 1983. IP addresses are the globally unique numeric identifiers necessary to distinguish individual entities that communicate over the Internet. The global demand for IP addresses has grown exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet, resulting in the exhaustion of readily available IPv4 addresses in all regions of the world. This transition, which will include ensuring IPv6 compatibility in the acquisition of new software/hardware, provides TSA a more manageable and secure network, as well as accommodating the expected growth in internet of things devices including checkpoint equipment and remote sensors. The requested funding will allow TSA to meet the milestones set out in the OMB memorandum M-21-07 dated November 19, 2020.

Additionally, the IT O&M vendor contract, IMPACT II, has been awarded and the transition has begun. IMPACT II will provide TSA with all infrastructure sustainment and IT support services for all technologies in the TSA IT environment, including 24x7x365 O&M support, Program and Project Management support activities, Information Assurance services, site and helpdesk support services, management of technology service providers (data center, network, application development, cloud services), and integration of all infrastructure changes.

- **Workforce:** ITIP will continue to transform the IT workforce with the skills and knowledge to maintain pace with new technologies, will drive the TSA mission through modernization of IT, will ensure a high level of employee job satisfaction, and will maintain enough skilled workers to accomplish the mission, while developing IT leaders for the future. As part of IT organizational objectives, TSA will provide a continuous learning environment for IT staff and all TSA staff, instructing how modern technology can facilitate an effective workforce and establish the knowledge and capabilities around operational technologies.
- **User Experience:** ITIP will continue the delivery of applications that enhance user experience/customer service/business operations by providing information that is easily applicable to the user. In addition, as part of IT organizational objectives, ITIP will emphasize data empowered decision making by creating a powerful data platform with business intelligence and advanced analytic capabilities that democratize data/data analytics to provide insight in decision making. Furthermore, ITIP will advance IT objectives for customer experience driven solutions by providing best-in-class customer service to all that utilize IT services while fully engaging in the TSA mission in all areas.

Figure A48: ITIP Funding Profile

ITIP – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 – FY 2028 Total**
ITIP	$391.9	$396.1	$396.9	$398.1	$399.0	$1,982.0
Total ITIP	**$391.9**	**$396.1**	**$396.9**	**$398.1**	**$399.0**	**$1,982.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

2. Field Information Systems (FIS)

FIS Capability Overview: The TSA FIS Capability Management mission area is responsible for collaborating with stakeholders to develop integrated materiel and non-materiel solution approaches to support secure integrated enterprise information management capabilities that are based on traceable and robust requirements with clear roadmaps towards fully integrated set of information systems and processes.

Integrated secure enterprise information systems are designed, developed, and implemented in order to support real-time information management and information-sharing for domestic and international airport operations management, mission management, risk management, compliance, and business analytics that allow real-time decision making. The primary focus areas of the current FIS mission space are as follows:

- Mobile Security Information Management;
- Field Data Modernization;
- Screening Operations Information Management Modernization; and,
- LE/FAMS Mission Scheduling Notification System (MSNS).

The narrative below will focus on STIP and MSNS Modernization.

Figure A49: FIS Capability Funding Profile

FIS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 – FY 2028 Total**
STIP	$16.8	$17.2	$17.2	$17.2	$17.2	$85.6
MSNS Modernization	$4.8	$4.8	$4.8	$4.8	$4.8	$24.0
MSNS Legacy	$15.7	$15.7	$15.7	$15.7	$15.7	$78.5
Field Information System PE	$0.8	$0.8	$0.8	$0.8	$0.8	$4.0
Total FIS	**$38.1**	**$38.5**	**$38.5**	**$38.5**	**$38.5**	**$192.1**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

i. STIP

Overview: STIP is authorized directly by the Aviation and Transportation Security Act of 2001 (Public Law 107-71) Title I Secs. 101, 105, and 109, which mandates TSA screening requirements. 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.

Future State: At the end of FY 2023, it is anticipated that there will be over 2,500 units of STIP-enabled TSE connected to TSA-Net. In FY 2024, 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 that are demonstrated or deployed to the field. These capabilities include emerging biometrics technology, remote maintenance, and/or support of current and future cybersecurity posture without disruptions to airport operations.

TSA must address the need for updated computing and data architecture elements as it develops and deploys machine-learning algorithms and advanced system data analytics and visualization capabilities. TSA will develop and test an updated computing and data architecture that addresses physical security and cybersecurity requirements. Further, the computing and data processing approaches will support the use of system performance data visualization and other system-level data analytics. STIP will support multimodal transportation screening operations, will provide uninterrupted support at checkpoints and checked baggage sites, and will be aligned to support self-service passenger-screening technologies when they are defined.

Figure A50: STIP Funding Profile

STIP – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
STIP	$16.8	$17.2	$17.2	$17.2	$17.2	$85.6
Total STIP	**$16.8**	**$17.2**	**$17.2**	**$17.2**	**$17.2**	**$85.6**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

ii. MSNS Modernization

Overview: MSNS facilitates coordination of air marshal availability and communication of mission assignments with the FAMS field offices and air marshals, providing mission-planning capabilities for FAMS Flight Operations personnel. MSNS assigns air marshals to flights according to TSA's risk-based security strategy, books airline and hotel reservations, and tracks mission execution.
MSNS uses a total of nine systems, with a core legacy application exclusively designed for airline crew management. Over time, this legacy system has left a gap in software capability that otherwise could incorporate an expansion of mission-planning requirements, including consideration of threat information and evolving global terrorist threats. The resulting gap in real-time data access is filled by numerous manual processes that protect information that is sensitive to the FAMS mission, responds to critical intelligence, and meets increased schedule coordination requirements. Current scheduling technology cannot be configured to meet TSA's risk-based security and counterterrorism objectives. As a result, mission planners must make significant manual interventions to meet requirements.

Future State: FAMS will continue to operate its legacy applications; however, a modernized MSNS, toward which funds within the profile are dedicated, will facilitate the redistribution of

personnel to streamlined automated processes that reduce personnel requirements and decrease calendar time required to publish a FAMS mission roster. Scheduling modernization also increases the number of possible missions that the FAMS will be able to fly, providing mission planners with greater flexibility. Replacement of the obsolete Sabre Aircrews scheduling software, re-architecture, re-imagination, and integration of the remaining eight MSNS applications also will contribute to a more automated process.

TSA seeks to modernize systems with broader access to include scalable solutions and integration and standardization of data and information. Modernization also demands that TSA identifies cyber challenges early in the requirements development lifecycle.

Key focus areas include the development of the Aviation Security Architecture, sponsoring a capability analysis review of the data integration for screening operations, field information systems, and development of mobile information management capabilities to support the checkpoint operating environment for TSOs and LE/FAMS.

Figure A51: MSNS Funding Profile

MSNS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
MSNS Modernization	$4.8	$4.8	$4.8	$4.8	$4.8	$24.0
Total MSNS Modernization	**$4.8**	**$4.8**	**$4.8**	**$4.8**	**$4.8**	**$24.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

Future of the FIS Capability: In partnership with stakeholders across TSA, DHS Components, and industry stakeholders, FIS is engaging in initiatives underway to modernize systems with broader access to scalable solutions and in integration and standardization of data and information, and is ensuring that cyber challenges are identified early in the requirements development lifecycle.

Key focus areas include the development of the Aviation Security Architecture, sponsoring a capability analysis review of the data integration for screening operations, field information systems, and development of mobile information management capabilities to support the checkpoint operating environment for TSOs and LE/FAMS.

3. Enterprise Physical Access Control System (ePACS)

Overview: The ePACS is a system that complies with 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 OMB 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 this end, DHS has mandated the integration of all components' PACS as part of the DHS PACS Modernization initiative.

Figure A52: ePACS

TSA facilities currently rely on standalone configured PACS that operate only at the local site level. The local TSA end users have to add, remove, and adjust personnel roles and access manually in their PACS. The TSA Physical Security Office is implementing a nationwide end-to-end HSPD 12-compliant ePACS solution for all field locations that operate on the Field Security Network. This enterprise solution will integrate with TSA's existing nationwide local area network/wide area network (TSANet) in order to communicate with the already-established Federal Bridge Certification Authority, which consists of a collection of public key infrastructure components (e.g., certificate authorities, directories, certificate policies, and certificate practice statements) that are used to provide certificate holder interoperability.

To migrate TSA facilities successfully to ePACS, the TSA Physical Security Office relies on the nationwide security contract to assess, provide upgrade installs, and 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 2022, 95 locations have migrated to ePACS, and 94 TSA locations are planned for migration in FY 2023 and FY 2024. The cost for the ePACS implementation and maintenance is $14.5 million per year, until 600 TSA facilities have migrated to ePACS.

Future State: ePACS will continue supporting and migrating PACS for all TSA-owned and/or -leased facilities. TSA continues to partner and engage with the DHS Office of the Chief Security Officer, industry technical experts, and other federal agencies in support of this initiative. DHS is implementing the PACS Modernization Working Group Charter, which will advise TSA on emerging physical access control methods for updates within the HSPD-12 program. The working group will evaluate the current physical access control technologies against the needs for future access control management to provide recommendations to the HSPD-12 Governance Committee.

Figure A53: ePACS Funding Profile

ePACS – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
ePACS	$14.6	$14.6	$14.6	$14.7	$14.7	$73.2
Total ePACS	**$14.6**	**$14.6**	**$14.6**	**$14.7**	**$14.7**	**$73.2**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

4. Human Capital (HC) IT Modernization Personnel Futures Program

Overview: The Personnel Futures Program (PFP) provides end-to-end human capital (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, and to bring the storage and processing of sensitive personally identifiable information for candidates and employees into secure cloud computing environments.

HC modernization is implementing a hybrid solution, consisting of both on-premises and cloud technology. The modernization will maximize efficiency through the use of software-as-a-service, robotic process automation, and machine-learning.

PFP expects leveraged technologies to show trends of realized operational efficiencies. User Self-Service will improve quality and reduce time to process candidate forms and personnel transactions. HC modernization will continue to support an innovative workforce through the Office of Personnel Management's USA Staffing, providing TSA with an integrated talent acquisition system; the Careers Website, providing clear and transparent information to applicants about career opportunities; the User Interface Path, providing automated reviews of Electronic Questionnaires for Investigations Processing; ServeU, providing users an integrated personnel a payroll system; and cloud computing, providing security for a mobile and remote workforce.

Future State: By FY 2024, this self-service and artificial intelligence automation will empower employees to manage their HC process and elections. Human Capital training and business process and systems will continue undergoing a modernization effort to bring the storage and processing of sensitive personally identifiable information for candidates and employees into secure cloud-computing environments.

By FY 2025, the modernization is on track to continue enhancement of operational processes and to improve the overall customer experience. The commercially available customer relationship management platform and applications implemented into the environment in FY 2023 will be used further to expand self-service capabilities, to integrate with other hiring process partners, to transform performance management, and to extend personnel process automation to payroll and benefits transactions, delivering state-of-the-art capabilities across the enterprise.

Figure A54: HC IT Modernization PFP Funding Profile

HC IT Modernization PFP – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
PFP - Mission Support	$127.9	$127.9	$127.9	$127.9	$127.9	$639.5
PFP - Screener Training and Other	$14.6	$14.6	$14.6	$14.6	$14.6	$73.0
Total HC IT Modernization PFP	**$142.5**	**$142.5**	**$142.5**	**$142.5**	**$142.5**	**$712.5**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

5. Staffing, Scheduling, Time, and Attendance System (SSTA)

Overview: The SSTA system supports almost 50,000 TSOs. Details of the program include:

- Electronic Time, Attendance, and Scheduling (eTAS) is an implementation of the commercially-available technology for the management of TSO schedules, and time and attendance. The customization is based on TSA pay codes, TSA payroll policy, and the Collective Bargaining Agreement;
- The Shift and Leave Bid modules on TSA's web platform comprise Scheduling, Management, and Resource Tasking (SMART). The application permits TSOs to bid remotely on both annual leave and shifts, per Collective Bargaining Agreement guidelines;
- Currently, SMART is integrated with eTAS to streamline data sharing between the subsystems; and,
- Enhanced Staffing Model (ESM) is a system used for resource forecasting and allocation. It uses volume projections, rates and standards, and passenger modeling and simulations to determine how many TSOs are required at each airport checkpoint. The system is in O&M and is being used nationwide.

Future State: SSTA provides a standardized system for scheduling across all airports, allowing seamless data exchange and an automated workflow. The goal is to integrate TSA's scheduling and time and attendance systems to provide an effective and quick path to production capability. These systems include: SMART, eTAS, ESM, and a new Optimization Tool under a single workflow process. It will manage staff and resource requirements in the near-term based on resource availability and predicted changes in travel patterns and will allow TSOs access to SSTA from their personal mobile devices. SSTA will replace current clocks that are at end-of-life, provide employees with self-service scheduling and time and attendance capabilities, and will increase visibility and management of resources and operations at airports.

TSA envisions SSTA as a hybrid cloud solution that will assist TSOs in performing time, attendance, scheduling, and budget functions at federalized airports.

Figure A55: SSTA System Funding Profile

SSTA System – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
eTAS - Investment	$3.7	$3.7	$3.7	$3.7	$3.7	$18.5
SSTA System - Non-Investment	$12.7	$12.7	$12.7	$12.7	$12.7	$63.5
Total SSTA System	**$16.4**	**$16.4**	**$16.4**	**$16.4**	**$16.4**	**$82.0**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

6. Air Cargo IT Systems

Overview: PLEASE REFER TO AIR CARGO SECURITY TECHNOLOGY PROGRAM (Sec. B. Threat Detection SoS, sub-Section 5. MPAC).

Future State: PLEASE REFER TO AIR CARGO SECURITY TECHNOLOGY PROGRAM (Sec. B. Threat Detection SoS, sub-Section 5. MPAC).

Figure A56: Air Cargo IT Systems Funding Profile

Air Cargo IT Systems – FY 2024 - FY 2028 ($ in millions)						
	FY 2024	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2024 - FY 2028 Total**
Air Cargo Security Portfolio - Investment[21]	$13.3	$13.3	$13.3	$13.3	$13.3	$66.5
Total Air Cargo IT Systems	**$13.3**	**$13.3**	**$13.3**	**$13.3**	**$13.3**	**$66.5**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

[21] Air Cargo Security Portfolio includes the Performance and Results Information Systems (PARIS) investment that supports Air Cargo, at $114K per year, FY 2024 – FY 2028.

II. PSP Legacy Program Funding Profile

The PSP Legacy program contains four technologies (BLS, BPS, CAD, and WTMD). Changes to this PSP cost driver in FY 2023 reflected a realignment of Capabilities Development to the Mission Support program/project/activity, in addition to increases to the agency's Federal Employees Retirement System contribution, and the 2023 pay raise.

Figure A57: PSP Legacy Funding Profile

Passenger Screening Program Legacy – FY 2024 - FY 2028 ($ in millions)						
	FY 2023	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-FY 2027 Total**
BPS	$0.9	$0.9	$0.9	$0.9	$0.9	$4.5
BLS	$1.7	$1.4	$1.4	$1.5	$1.4	$7.4
WTMD	$3.3	$3.4	$3.4	$3.4	$3.5	$17.0
CAD	$0.8	$0.8	$0.8	$0.8	$0.8	$4.0
Integrated Logistics Support (ILS) Maintenance	$12.3	$12.3	$12.3	$12.3	$12.3	$61.5
Total PSP Legacy	**$19.0**	**$18.8**	**$18.8**	**$18.9**	**$18.9**	**$94.4**
FY 2024 reflects the President's Budget, and FY 2025 - FY 2028 are estimated amounts.						

III. Technology Acquisitions

TSA has updated what was formerly the Transportation Security Acquisition Manual, signed in August 2018, to be titled the TSA Acquisition Manual (TSAAM). The TSAAM aligns to DHS guidance regarding implementation of the Acquisition Lifecycle Framework (ALF),[22] which outlines key activities for defining, developing, and delivering needed capabilities. In accordance with DHS Acquisition Management Instruction 102, it outlines the high-level, structured approach to define, develop, and deploy capabilities in the TSA ALF. TSAAM components combine to outline a repeatable, transparent, and flexible process that TSA uses when pursuing a new acquisition.

As the leadership of a TSA ALF Integrated Product/Project Team begins the process of structuring a prospective acquisition, the TSAAM guides decision-making and organizational activities. It also assists execution-level members of the ALF Integrated Product/Project Team to understand their responsibilities and required actions over the lifecycle of the acquisition, as well as those of their peers. Lastly, it enables TSA leadership to make approval decisions based on robust understanding of key decision points, processes, and stakeholders. As a keystone manual for TSA acquisitions, it provides the foundational information that acquisition teams need to deliver the right capability at the right time through a series of acquisition lifecycle phases.

A. Acquisition Lifecycle

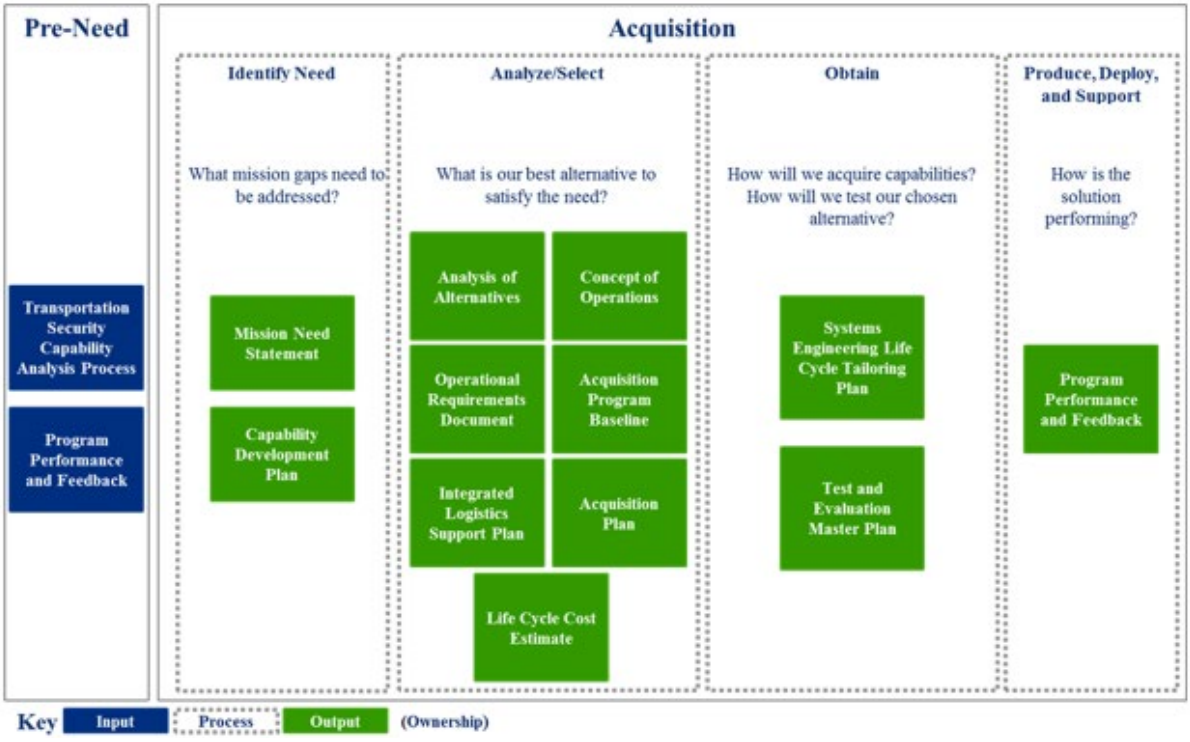
Aligning Resources in Pre-Need

The Pre-Need Phase is a prerequisite for entering the ALF. In this phase, TSA collects, analyzes, and prioritizes TSA capability gaps. It also includes an analysis of TSA resources, a risk assessment, and a capability analysis. The capability analysis includes the Transportation Security Capability Analysis Process (TSCAP), which analyzes TSA's capability gaps to identify recommended courses of action for well-timed gap prioritization decisions. If the only acceptable course of action after gap identification and prioritization is to implement a material solution (a new device or significant modifications to existing devices), TSA continues through the ALF into the Identifying Need Phase.

Figure A58 shows the subsequent phases of the lifecycle that TSA will execute to acquire a material solution.

[22] 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).

Figure A58: Overview of the Acquisition Lifecycle for Security-related Technology (SRT) Material Solutions



Identifying Needs

After the Pre-Need Phase has concluded in a recommendation for a material solution such as SRT, TSA transitions into the Identifying Needs Phase of the Acquisition Lifecycle. 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

In the Analyze and Select Phase, TSA screens capabilities and analyzes the results to select prospective solutions. 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 approve or disapprove officially a prospective acquisition.

Leveraging Department Efficiencies

As TSA moves into the Obtain Phase, it first considers how to leverage 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, to reduce redundancy, to drive standardization, to streamline procurements, and to improve business efficiency.

Obtaining Capabilities

In the Obtain Phase, TSA focuses on systems development, testing, and evaluation to ensure an effective acquisition. TSA has made strides over the past few years to accelerate capability delivery and to reduce cost while obtaining solutions. Below, TSA has provided updates for initiatives with significant status changes:

- **Accelerating Capability Delivery and Reducing Cost:** Since 2018, DHS has changed acquisition policy, and TSA has updated the TSAAM to reflect these changes and to ensure that processes comply with current DHS acquisition guidelines. Specifically, TSA has updated requirements in DHS Management Instruction 102-01, including instructions for acquisition management, cybersecurity, DHS agile methodology, and rapid acquisition guidelines. These changes will allow TSA to maximize cost-effectiveness throughout the ALF and to accelerate capability delivery.
- **Improving Agile Processes:** In addition to revising ALF requirements, TSA has updated the TSAAM to clarify how TSA stakeholders should engage with ALF processes. For example, to address a previous lack of understanding among stakeholder groups, the definition of Transition Manager now clearly states the responsibilities for Transition Managers across the ALF. Additionally, TSA redefined the relationship between CMs and program managers to clarify roles across the development of a capability. These changes not only will define transition points between stakeholder roles and responsibilities, but they also will improve coordination of requirements for each phase of the ALF. As a result, the likelihood of delays or disruptions to capability delivery because of lack of stakeholder coordination or clear roles and responsibilities will be reduced.

  Furthermore, TSA updated the TSAAM to require integration with IT stakeholders, codifying IT integration points and reviews to ensure IT engagement across the ALF. This update also included IT-specific enhancements like cybersecurity requirements throughout the TSAAM and incorporated agile IT processes, among the other agile process additions to the document. These changes support integration of an IT-specific acquisition framework and drive general process improvement.
- **Accelerating Capability Delivery in Response to COVID-19:** The COVID-19 pandemic response and recovery shifted and accelerated many of TSA's priorities for obtaining new capabilities through the ALF process. Accordingly, TSA updated the TSAAM to accelerate capability delivery through several acquisition processes. To begin, the Urgent Solution Intake Process has been updated to define a standardized evaluation process to vet technology solution proposals that address urgent mission needs rapidly and to integrate existing solution intake channels. Additionally, these updates define a starting point to initiate outreach with appropriate stakeholders and to provide users with baseline criteria to identify suitable acquisition and procurement pathways. Finally, the updates ensure a 90-day procurement process by requiring prioritization of the procurement and by concentrating contracting resources. These newly defined steps to award a contract rapidly allow TSA to meet mission requirements under critical circumstances, as determined by TSA leadership.

IV. Compliance Matrix

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 222 of the FY 2023 DHS Appropriations Act (P.L 117-103) and its accompanying Joint Explanatory Statement; and by the Transportation Security Acquisition Reform Act (P.L. 113-245)). The table below shows where in the CIP the requirements are discussed.

Figure A58: 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 SRT.	*Transforming Mission Execution* – Identifying and Prioritizing Threats, Risks, and Capability Needs and Gaps
d(1)	The plan shall include consideration of the most recent Quadrennial Homeland Security Review.	Most recent Quadrennial Homeland Security Review was released in 2014.
d(2)B	The set of SRT acquisition needs shall include planned technology programs and projects with defined objectives, goals, timelines, and measures.	*Transforming Mission Execution* – Executing Our Mission *Appendix* – 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.	*Strategic Priorities to Drive Transformation* *Transforming Mission Execution*
d(4)	The plan shall include an identification of currently deployed SRTs that are at or near the end of their lifecycles.	*Appendix* – 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* – Capital Investment Programs
d(6)	The plan shall include identification of opportunities for public-private partnerships.	*Transforming Mission Execution* – Partnering to Accelerate Action
d(6)	The plan shall include identification of opportunities for small and disadvantaged company participation.	*Transforming Mission Execution* – Partnering to Accelerate Action
d(6)	The plan shall include identification of opportunities for intragovernment collaboration.	*Transforming Mission Execution* – Research and Development; Partnering to Accelerate Action
d(6)	The plan shall include identification of opportunities for university centers of excellence.	*Transforming Mission Execution* – Partnering to Accelerate Action
d(6)	The plan shall include identification of opportunities for national laboratory technology transfer.	*Transforming Mission Execution* – Research and Development; Partnering to Accelerate Action

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.	*Transforming Mission Execution* – Partnering to Accelerate Action *Appendix*– Capital Investment Programs
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.	*Transforming Mission Execution* – Executing Our Mission
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.	*Appendix* – Technology Acquisitions
d(10)	The plan shall include an impact assessment to commercial aviation passengers.	*Transforming Mission Execution* – Executing Our Mission
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.	*Transforming Mission Execution* – Identifying and Prioritizing Threats, Risks, and Capability Needs and Gaps *Appendix* – Technology Acquisitions
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.	*Transforming Mission Execution* – Executing Our Mission*;* Defining a Future State; Research and Development

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 R&D investment trends within the public and private sectors.	*Transforming Mission Execution* – Research and Development
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.	*Transforming Mission Execution* – Partnering to Accelerate Action
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.	*Transforming Mission Execution* – Executing Our Mission *Appendix* – 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 2022 – FY 2026 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.	*Appendix* – TSE Acquisition Update

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.	*Transforming Mission Execution* – Executing Our Mission *Appendix* – Capital Investment Programs

V. Abbreviations

Abbreviation	Definition
3D	Three-Dimensional
3PK9-C	Third-Party Canine Cargo Screening
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
ASCF	Aviation Security Capital Fund
ASL	Automated Screening Lane
AT	Advanced Technology
BLS	Bottled Liquid Scanner
BPS	Boarding Pass Scanner
CAP	Capability Acceptance Process
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
CPAM	Checkpoint Automation
CPSS	Checkpoint Property Screening System
CT	Computed Tomography
C-UAS	Counter-Unmanned Aerial System
DHS	Department of Homeland Security
DI	Digital Identity
DICOS	Digital Imaging and Communications in Security
DTI	Detect, Track, and Identify
EBSP	Electronic Baggage Screening Program
EDC	Explosives Detection Canine
EDS	Explosive Detection System

Abbreviation	Definition
EMD	Enhanced Metal Detector
EO	Executive Order
ePACS	Enterprise Physical Access Control System
eTAS	Electronic Time, Attendance, and Scheduling Tool
ETD	Explosives Trace Detection
FAA	Federal Aviation Authority
FAMS	Federal Air Marshal Service
FAST	Flexible Agile Scalable Teams
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
IAMCS	Indirect Air Carrier Management System
ICAO	International Civil Aviation Organization
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
LEO	Law Enforcement Officer
LFA	Lead Federal Agency
LGA	Liquids, Gels, and Aerosols
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
NRT	Near Real-Time
OA	Open Architecture
O&M	Operations and Maintenance

Abbreviation	Definition
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
PSP	Passenger Screening Program
PVS	Primary Viewing Station
R&D	Research and Development
RAPID	Real-Time Analytic Platform for Incident Deterrence
RTSPA	Risk and Trade Space Portfolio Analysis
S&T	DHS Science and Technology Directorate
SLTT	State, Local, Tribal, and Territorial
SoS	System of Systems
SRT	Security-Related Technology
SST	Surface Security Technology
SSTA	Staffing, Scheduling, Time, and Attendance
STAT	Security Threat Assessment Tool
STIP	Security Technology Integration Program
STSTAC	Surface Transportation Security Advisory Committee
TAZ	TSA Azure
TDC	Travel Document Checker
TRL	Technology Readiness Level
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
ZTA	Zero Trust Architecture