Capital Investment Plan

FY 2023–FY 2027

July 26, 2022

Fiscal Year 2022 Report to Congress

Homeland Security

Transportation Security Administration

Message from the Administrator

July 26, 2022

I am pleased to present the following "Capital Investment Plan" (CIP) for Fiscal Year (FY) 2023–FY 2027, which was prepared by the Transportation Security Administration (TSA).

TSA compiled the CIP according to reporting requirements in Section 222 of the FY 2022 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-103) and its accompanying Joint Explanatory Statement, in Senate Report 115-283 accompanying the FY 2019 DHS Appropriations Act (P.L. 116-6), and in 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 provided to the following Members of Congress:

The Honorable Rosa L. DeLauro
Chairwoman, House Committee on Appropriations

The Honorable Kay Granger
Ranking Member, House Committee on Appropriations

The Honorable Patrick J. Leahy
Chairman, Senate Committee on Appropriations

The Honorable Richard C. Shelby
Vice Chairman, Senate Committee on Appropriations

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

The Honorable John Katko
Ranking Member, House Committee on Homeland Security

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

The Honorable Roger F. Wicker
Ranking Member, Senate Committee on Commerce, Science, and Transportation

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2801, or TSA's Legislative Affairs office at (571) 227-2717.

Sincerely,

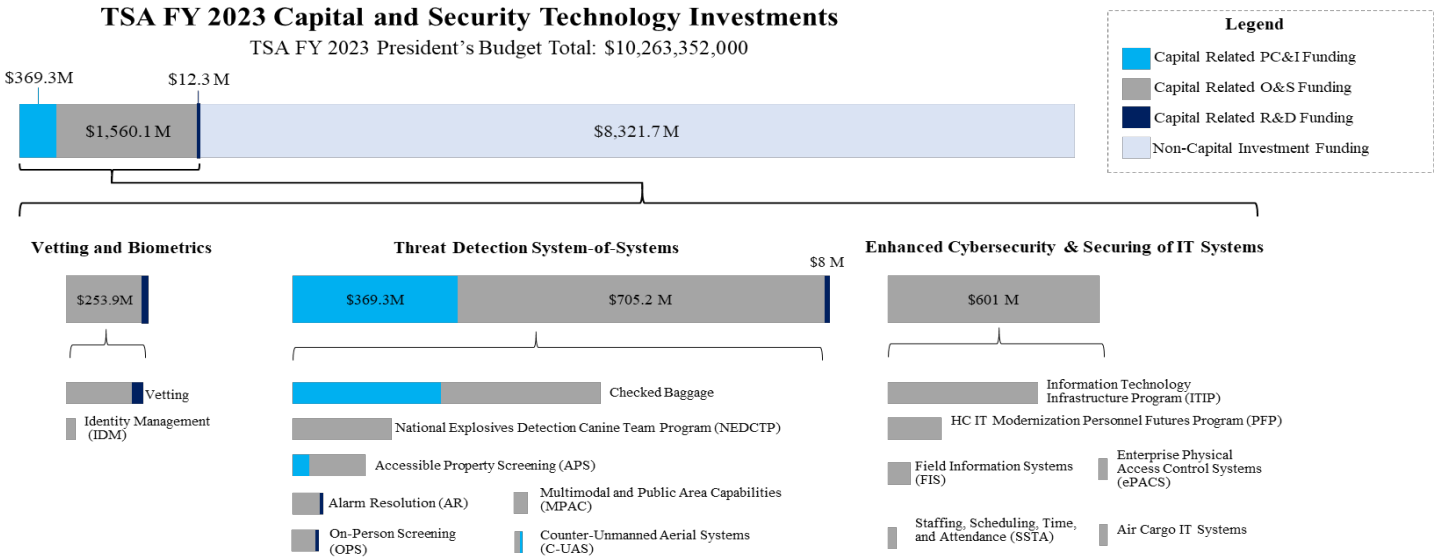
David P. Pekoske
Administrator

Executive Summary

Harnessing innovative technology is a major priority for DHS. While personnel are critical to the success of capital investments, the CIP for FY 2023–FY 2027 outlines TSA's strategy for continuous and sustained investment in new, and the replacement of obsolete, TSE and other transportation security solutions. 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 invest in, acquire, and field new technologies and enhanced secure information technology (IT) systems to strengthen security effectiveness and efficiency.

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, 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. 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

[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 do not shift in line with TSA's changing priorities through the annual budget process.

priorities; adapt to disruptions in the transportation ecosystem; and address complex future challenges within the FYHSP. **Figure 2** outlines TSA's FY 2023 budget request.

Figure 2: TSA Budget Request FY 2023

TSA Budget Request FY 2023 Congressional Justification ($ in thousands)								
	FY 2021 Enacted		FY 2022 Enacted		FY 2023 President's Budget		FY 2022–FY 2023 Total Changes	
	Full-time Equivalent (FTE)	$000	FTE	$000	FTE	$000	FTE	$000
Operations and Support (O&S)	56,210	$7,793,715	54,787	$8,091,193	57,033	$9,542,725	2,246	$1,451,532
Procurement, Construction, and Improvements (PC&I)	0	$134,492	0	$160,736	0	$119,345	0	($41,391)
Research and Development (R&D)	0	$29,524	0	$35,532	0	$33,532	0	($2,000)
Appropriated Funds	**56,210**	**$7,957,731**	**54,787**	**$8,287,461**	**57,033**	**$9,695,602**	**2,246**	**$1,408,141**
Vetting Fees - Discretionary	327	$353,964	386	$200,000	386	$311,750	0	$111,750
Mandatory Fees	19	$255,500	19	$256,000	19	$256,000	0	$0
Total Budget Authority	**56,556**	**$8,567,195**	**55,192**	**$8,743,461**	**57,438**	**$10,263,352**	**2,246**	**$1,519,891**
Less Mandatory Fees	-19	($255,500)	-19	($256,000)	-19	($256,000)	0	$0
Gross Discretionary	**56,537**	**$8,311,695**	**55,173**	**$8,487,461**	**57,419**	**$10,007,352**	**2,246**	**$1,519,891**
Less Discretionary Vetting Fees	-327	($353,964)	-386	($200,000)	-386	($311,750)	0	($111,750)
Appropriated Funds	**56,210**	**$7,957,731**	**54,787**	**$8,287,461**	**57,033**	**$9,695,602**	**2,246**	**$1,408,141**
9/11 Passenger Security Fee Offset	0	($212,243)	0	($2,110,000)	0	($4,012,443)	0	($1,902,443)
Net Discretionary	**56,210**	**$7,745,488**	**54,787**	**$6,177,461**	**57,033**	**$5,683,159**	**2,246**	**($494,302)**

Strategic Alignment

The CIP represents the output of TSA's efforts to plan for 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 2023–FY 2027 CIP follows priorities set by TSA's FY 2023–FY 2027 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 2023–FY 2027

DRAFT CIP - FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-FY 2027 Total**
A. Vetting and Biometrics						
I. Vetting	$220.1	$217.6	$215.3	$214.8	$214.4	**$1,082.2**
II. IDM	$33.8	$33.7	$33.7	$33.7	$33.7	**$168.6**
Vetting and Biometrics Subtotal	**$253.9**	**$251.3**	**$249.0**	**$248.5**	**$248.1**	**$1,250.8**
B. Threat Detection System-of-Systems						
I. APS	$230.2	$221.5	$221.6	$221.7	$221.7	**$1,116.7**
II. AR	$55.7	$55.1	$55.1	$55.2	$55.2	**$276.3**
III. OPS	$65.8	$66.5	$66.6	$66.6	$66.6	**$332.1**
IV. Checked Baggage	$520.8	$507.0	$507.2	$507.4	$507.5	**$2,549.9**
V. MPAC	$18.8	$18.8	$18.8	$18.8	$18.8	**$94.0**
VI. C-UAS	$11.2	$11.2	$11.2	$11.2	$11.2	**$56.0**
VII. NEDCTP	$180.0	$182.2	$184.0	$185.9	$187.8	**$919.9**
Threat Detection System-of-Systems Subtotal	**$1,082.5**	**$1,062.3**	**$1,064.5**	**$1,066.8**	**$1,068.8**	**$5,344.9**
C. Enhanced and Secure IT Systems						
I. ITIP	$385.2	$388.3	$389.6	$394.7	$391.3	**$1,949.1**
II. FIS	$31.8	$31.8	$31.8	$31.9	$31.9	**$159.2**
III. ePACS	$14.5	$14.5	$14.5	$14.6	$14.6	**$72.7**
IV. Human Capital (HC) IT Modernization PFP	$148.7	$145.0	$134.5	$133.5	$133.5	**$695.2**
V. SSTA System	$12.0	$12.0	$12.0	$12.0	$12.0	**$60.0**
VI. Air Cargo IT Systems	$13.2	$13.2	$13.2	$13.2	$13.2	**$66.0**
Enhanced and Secure IT Systems Subtotal	**$605.4**	**$604.8**	**$595.6**	**$599.9**	**$596.5**	**$3,002.2**
Total	**$1,941.8**	**$1,918.4**	**$1,909.1**	**$1,915.2**	**$1,913.4**	**$9,597.9**

FY 2023-FY 2027 reflects the FY 2023 Congressional Justification.

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 nonstandardized data, images, or interfaces, which forces TSA to rely on original equipment manufacturers (OEM) and existing contracting mechanisms for software, component, or operational upgrades. This reliance on OEMs for screening technology improvements 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 initiatives and R&D.

Open Architecture: TSA's introduction of open system software architecture elements into TSE is a pivotal investment in advancing TSA's future state. This type of architecture increases interoperability through the use of open standards and simplifies adding, changing, or replacing new components, and data sharing. Through open architecture, 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.

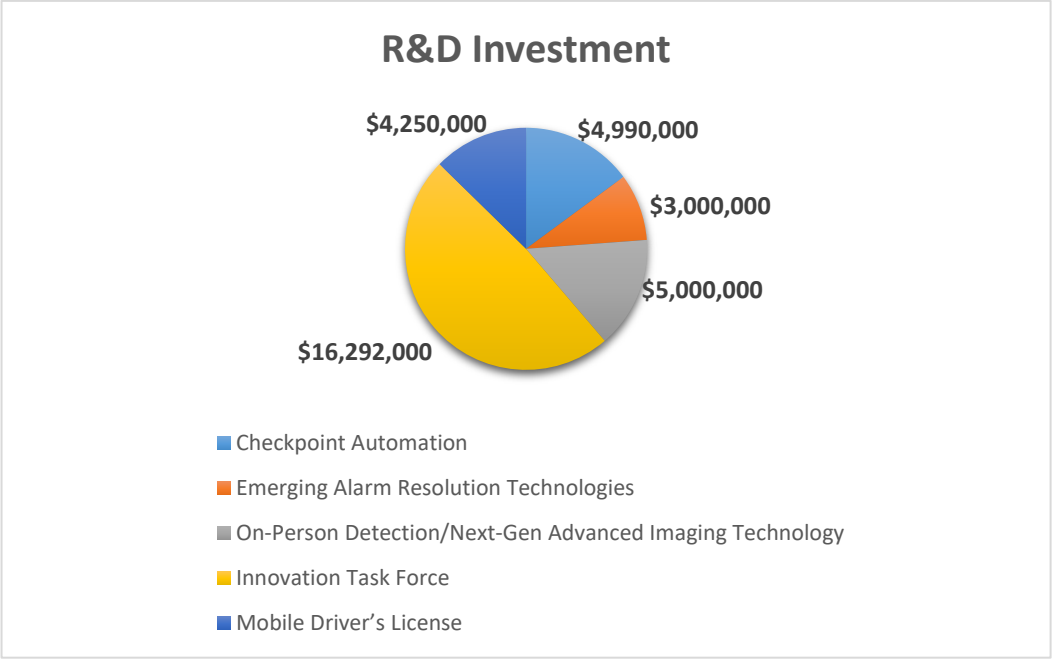
Open architecture also increases efficiency and interoperability across TSE and screening systems, advances risk-based security objectives, enables modularity, reduces costs, and expedites delivery of capabilities. Artificial intelligence and machine learning, through a number of methods including integrating advanced detection algorithms into screening equipment, has the ability to impact all of TSA's current operations positively. TSA must focus not only on capital investment, but also human talent, training, and capabilities to scale these solutions.

In coordination with other innovative acquisition methodologies, such as dual sourcing and competitive prototyping, open architecture increases competition for upgrades and subsystem level components. Similar to the Department of Defense's Modular Open Systems Approach, which seeks to develop joint combat capabilities, the TSA open system architecture supports a unified, international agreement for improved buying power, data sharing, and system capabilities at speed. TSA has established an open architecture environment through the Checkpoint Automation (CPAM) initiative to address these challenges and has defined "Open

Data" and "Standardization" as the key pillars to guide open architecture initiatives and to enable OEM and third-party implementation of best-of-breed solutions to address challenges rapidly.

R&D: In addition to the CPAM R&D work that supports Open Architecture, TSA's mission success depends on simultaneous investment in capital assets in R&D. This includes applied research, development, testing, and evaluation activities that advance innovative technology solutions and support TSA's security infrastructure. 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 2023 R&D funds is shown in **Figure 4**.

Figure 4: R&D Investment FY 2023



Capital Investment Plan
FY 2023–FY 2027

Table of Contents

I. Legislative Language

This report addresses reporting requirements in Section 222 of the Fiscal Year (FY) 2022 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-103) and its accompanying Joint Explanatory Statement; Senate Report 115-283 accompanying the FY 2019 DHS Appropriations Act (P.L. 116-6); and the Transportation Security Acquisition Reform Act (P.L. 113-245).

P.L. 117-103 states the following:

> **SEC. 222.** Not later than 30 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 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 222.** The agreement continues a provision requiring TSA to provide a report that includes the Capital Investment Plan, the five-year technology investment plan, and information on Advanced Integrated Passenger Screening Technologies.

Senate Report 115-283 provides:

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

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

SEC. 1611. 5-YEAR TECHNOLOGY INVESTMENT PLAN.

(a) IN GENERAL. —The Administrator shall—

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

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

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

(1) the Under Secretary for Management;

(2) the Under Secretary for Science and Technology;

(3) the Chief Information Officer; and

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

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

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

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

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

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

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

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

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

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

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

(7) an identification of the Administration's acquisition workforce needs for the management of planned security-related technology acquisitions, including consideration of leveraging acquisition expertise of other Federal agencies;

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

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

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

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

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

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

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

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

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

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

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

(1) an update of the Plan; and

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

II. Plan Overview

The 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) 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. The President's Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," in conjunction with the Office of Management and Budget's strategy to move the U.S. Government toward zero trust architecture, requires TSA to migrate to this 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.

Furthermore, following the President's EO 14058, "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government,"[2] 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.

Capital investments summarized in the CIP will transform TSA's execution of transportation security coupled with risk-based policy changes, process improvements, and strategic partnerships. 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 2023 President's Budget and outyear requirements in the Future Years Homeland Security Program (FYHSP).

[2] Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government | The White House

III. Strategic Priorities to Drive Transformation

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

- The TSA Strategy,[3] which articulates the shared vision, goals, and priorities for TSA through 2027;
- Administrator's Intent,[4] 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;[5] and
- The FY 2023–FY 2027 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 2023–FY 2027 requirements prioritization process, TSA considered the TSA Strategy and Administrator's Intent 2.0 and received briefs on mission/operational risk processes and capabilities from risk and capability, aviation forecasting, and intelligence subject matter experts. 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.

[3] TSA Strategy, 2018–2026: https://www.tsa.gov/sites/default/files/tsa_strategy.pdf
[4] Administrator's Intent 2.0 2020: https://www.tsa.gov/sites/default/files/tsa-administrators-intent-2.0.pdf
[5] 2020 Biennial National Strategy for Transportation Security: https://www.dhs.gov/publication/2020-biennial-national-strategy-transportation-security

IV. Transforming Mission Execution

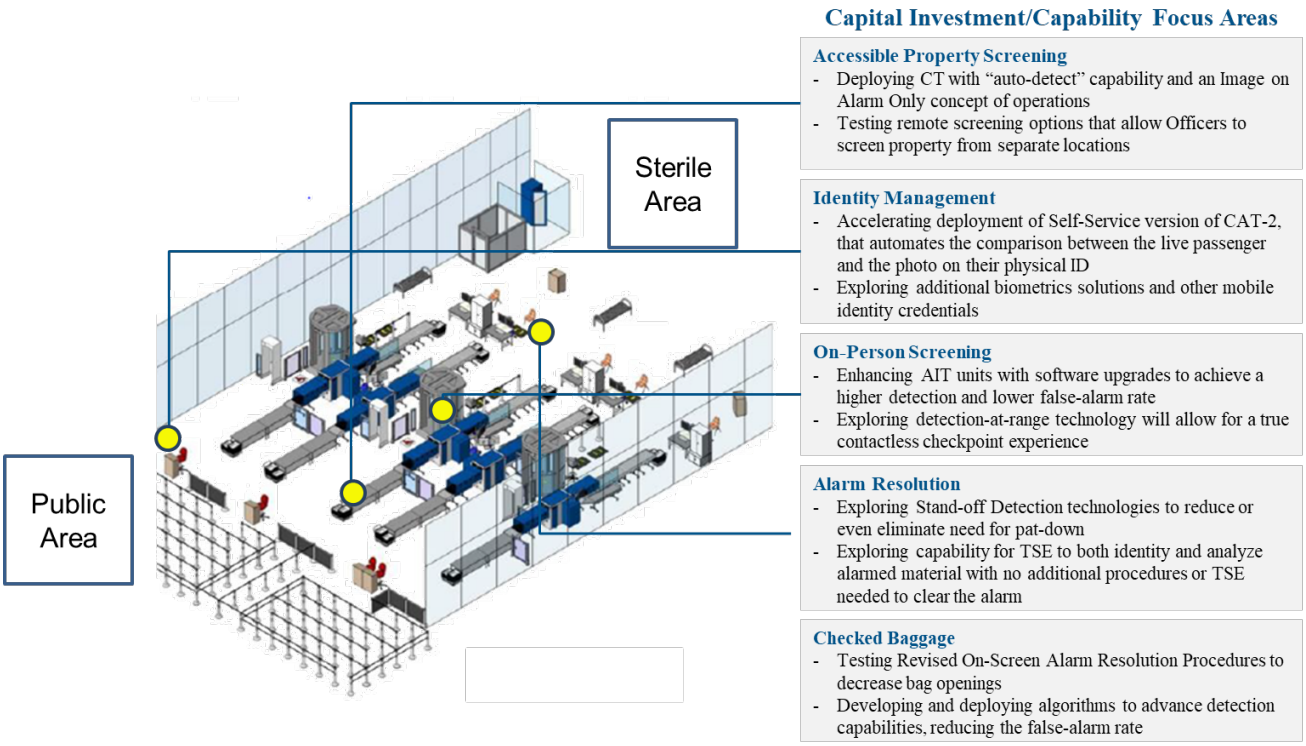
The transportation ecosystem continues to evolve with new and dynamic threats and other unpredictable disruptions, including the lingering impacts of the Coronavirus Disease 2019 (COVID-19) pandemic and cybersecurity threats from state and nonstate actors. Reflective of such, TSA must adapt to change 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.

The COVID-19 pandemic was a major disruption to all forms of transportation, but specifically the aviation ecosystem, which required drastic and rapid changes to the operational environment of security checkpoints. TSA responded by accelerating existing plans to transform checkpoints and to enhance security, prioritizing contactless and remote screening, both to ensure the integrity of aviation security and the safety of the traveling public and TSA's field officers. The pandemic heightened existing needs for TSA to evolve its approach to security screening, checkpoint design, and airport operations to reduce contact, to create a more seamless interconnected checkpoint experience, and to improve security measures.

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



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 systemwide 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.

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 system-of-systems. Current CMs support TSA's fielded capabilities and include most of TSA's capital investment programs.

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, 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.

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 in 2018 and its Identity Management Roadmap in 2022 to detail the agency's plan to evolve IDM into a more formalized and integrated capability across the enterprise. For example, TSA is developing 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.

TSA is piloting and testing a facial identification solution 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, recognized because of COVID-19 and future health impacts, 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 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: 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.

Figure 6 shows the funding aligned to vetting and biometrics projects and programs from the FY 2023 Congressional Justification (CJ) and TSA's FY 2023–FY 2027 FYHSP. Security-related technology (SRT)[6] programs are noted for traceability requirements in the 5-year technology investment plan requirements.

Figure 6: Vetting and Biometrics FY 2023–FY 2027

Vetting and Biometrics – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023– FY 2027 Total**
Vetting & Credentialing System	$85.1	$81.6	$78.6	$77.3	$76.1	$398.8
Secure Flight	$135.0	$136.0	$136.7	$137.5	$138.3	$683.5
Total Vetting	**$220.1**	**$217.6**	**$215.3**	**$214.8**	**$214.4**	**$1,082.3**
CAT	$26.1	$26.1	$26.1	$26.1	$26.1	$130.5
Identity Investment	$3.0	$3.0	$3.1	$3.1	$3.1	$15.3
Boarding Pass Scanner	$0.4	$0.3	$0.3	$0.3	$0.3	$1.5
Subtotal O&S	**$29.5**	**$29.4**	**$29.4**	**$29.5**	**$29.5**	**$147.3**
Subtotal PC&I	**$0.0**	**$0.0**	**$0.0**	**$0.0**	**$0.0**	**$0.0**
Mobile Driver's License	$4.3	$4.3	$4.3	$4.3	$4.3	$21.3
Subtotal R&D	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$21.3**
Total IDM	**$33.8**	**$33.7**	**$33.7**	**$33.7**	**$33.7**	**$168.6**
Total Vetting and Biometrics	**$253.9**	**$251.3**	**$249.0**	**$248.5**	**$248.2**	**$1,250.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

[6] 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.

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.

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'[7] 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 open architecture 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. 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. These enhancements will improve the passenger experience and will advance security by achieving a higher detection and lower false-alarm rate. As a result, TSA's move to contactless screening will be accelerated as the need for physical pat-downs decreases while extending AIT to all airports to the maximum extent possible. TSA is updating AIT units with advanced algorithms, including low probability of false alarm[8] and Gender-Neutral, to achieve these milestones. This is in line with the President's EO 13988, "Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation."[9] TSA is

---

[7] 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.

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

[9] Executive Order on Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation | The White House

applying open architecture concepts to integrate the advanced algorithms through the use of DICOS and OPSL, which will enable long-term capabilities consistent with CPSS.
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. Regarding checked baggage, TSA continues to work toward its goal of better detection of threat materials, lower threat mass, lower false-alarm rates, and lower lifecycle costs. As part of this work, DICOS provides standard image formatting across vendor solutions while Threat Recognition System allows for that integration of third-party algorithms.

Within the OPS capability, TSA continues exploring detection-at-range capabilities that focus on screening at speed and at distance to reduce contact, to improve integration, and to enhance the passenger experience.

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). 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.

Figure 7 shows the funding aligned to enhanced threat detection projects and programs from the FY 2023 CJ and TSA's FY 2023–FY 2027 FYHSP.

Figure 7: Threat Detection System-of-Systems FY 2023–FY 2027

Threat Detection System-Of-Systems – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023–FY 2027 Total**
APS	$124.8	$125.6	$125.7	$125.9	$126.0	$627.9
AR	$52.7	$52.1	$52.1	$52.2	$52.2	$261.3
OPS	$60.8	$61.5	$61.6	$61.6	$61.6	$307.1
Checked Baggage	$256.9	$257.0	$257.2	$257.4	$257.5	$1,286.0
Multimodal and Public Area Capabilities (MPAC)	$18.8	$18.8	$18.8	$18.8	$18.8	$94.0
C-UAS	$11.2	$11.2	$11.2	$11.2	$11.2	$56.0
National Explosives Detection Canine Team Program	$180.0	$182.2	$184.0	$185.9	$187.8	$919.9
Subtotal O&S	**$705.1**	**$708.5**	**$710.6**	**$712.8**	**$715.1**	**$3,552.2**
CPSS PC&I	$105.4	$95.9	$95.9	$95.8	$95.7	$488.7
Checked Baggage - Electronic Baggage Screening Program (EBSP) - Investment	$13.9	$0.0	$0.0	$0.0	$0.0	$13.9
Aviation Security Capital Fund - EBSP - Investment	$250.0	$250.0	$250.0	$250.0	$250.0	$1,250.0
Subtotal PC&I	**$369.3**	**$345.9**	**$345.9**	**$345.8**	**$345.7**	**$1,752.6**
Emerging AR Technologies	$3.0	$3.0	$3.0	$3.0	$3.0	$15.0
On-Person Detection/Next-Gen AIT	$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	**$1,082.5**	**$1,062.4**	**$1,064.5**	**$1,066.6**	**$1,068.8**	**$5,344.8**

FY 2023-FY 2027 reflects the FY 2023 CJ.

3. Enhanced Cybersecurity and Securing IT Systems

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. IT systems enhance existing and future procedures, operations, and technology, allowing TSA to ensure optimal security effectiveness and efficiency.

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. 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.

To optimize operational efficiency, TSA seeks to invest in modernizing existing mission support functions. The COVID-19 pandemic rapidly changed operational and staffing needs in the field, accelerating the need to modernize IT support functions. Modernizing HC and scheduling infrastructure like the Federal Air Marshal Service's Mission Scheduling and Notification System 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 2023 CJ and TSA's FY 2023–FY 2027 FYHSP.

Figure 8: Enhanced and Secure IT Systems FY 2023–FY 2027

Enhanced and Secure IT Systems – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-FY 2027 Total**
ITIP	$385.2	$388.3	$389.6	$394.7	$391.3	$1,949.1
Field Information Systems (FIS)	$31.8	$31.8	$31.8	$31.9	$31.9	$159.2
Enterprise Physical Access Control System	$14.5	$14.5	$14.5	$14.6	$14.6	$72.7
HC IT Modernization Personnel Futures Program	$148.7	$145.0	$134.5	$133.5	$133.5	$695.2
SSTA System	$12.0	$12.0	$12.0	$12.0	$12.0	$60.0
Air Cargo IT Systems	$13.2	$13.2	$13.2	$13.2	$13.2	$66.0
Total Enhanced and Secure IT Systems	**$605.4**	**$604.8**	**$595.6**	**$599.9**	**$596.5**	**$3,001.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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

TSA first identifies and assesses threats, risks, and capability needs and gaps to determine the capital investments required to advance TSA's strategic priorities and to execute the mission. Using intelligence reporting and analysis, modeling, and simulation capabilities, TSA calculates, ranks, and compares risks to the transportation sector, and provides TSA leadership with a comprehensive understanding of the transportation sector's terrorism and other risk landscapes. 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 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. Risk management approach must support TSA's ability to identify, analyze, and respond appropriately to strategic risks across the full spectrum of TSA activities.

2. Transportation Sector Security Risk Assessment (TSSRA)

TSSRA is an enterprise-level, crossmodal 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, the associated capability gap, 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**
  - *FISs:* Collaborating with field security operations stakeholders to innovate and advance FISs 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. Defining a 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 prioritizing emerging and interconnected technologies and will continue developing solutions that seamlessly connect the cyber-physical space. TSA's technology enhancements also will be informed by COVID-19 impacts on transportations systems, particularly in accelerating the need for investments in contactless and remote screening capabilities. 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.

1. Open Architecture

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 open architecture 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 Open Architecture for Airport Security Systems document.[10]

TSA has defined "Open Data" and "Standardization" as the key elements of the CPAM initiative to guide open architecture initiatives and to enable OEM and third-party implementation of best-of-breed solutions to rapidly address challenges. The following components of CPAM support TSA's achievement of its open architecture vision of the future:

- 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;
- 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.

2. CPAM Initiative

The CPAM initiative will lead 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 is a pivotal priority in advancing TSA toward the future state. Open architecture 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.

[10] Open Architecture for Airport Security Systems: Open Architecture for Airport Security Systems (aci-europe.org)

D. 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 5 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.

E. 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 open architecture 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.

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. For example, modernization initiatives are underway aimed at multiple legacy systems, such as the Performance and Results Information System and Global Risk Analysis and Decision Support System, that support the collection of data and performance across TSA. These initiatives will improve data integrity, reporting, and analysis. 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 law enforcement/Federal Air Marshal Service 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.

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 was shipped to the Transportation Security Lab 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 transportation security technologies and improvements to transportation 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 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)**

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 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 90 pieces of TSE and 3,000 ASL antimicrobial bins. It also has transitioned more than 90 urgent operational need ASLs for a total donation amount of more than $163 million through the first quarter of FY 2022. TSA is executing the CAP with 14 donors and is anticipating two additional donation projects in FYs 2022-2023.[11]

9. Surface Transportation Security Advisory Committee (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

[11] Current donors are George Bush Intercontinental Airport/United, Denver International Airport, Orlando International Airport/Greater Orlando Aviation Authority, LaGuardia Airport/Delta, Newark Liberty International Airport/Port Authority of New York and New Jersey, Los Angeles International Airport/Alaska, and Charlotte Douglas International Airport, with screening technologies that include AIT (14), ASL (16), and CPSS (34).

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, and nonvoting 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.

V. 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 aviation security, continued investment in the workforce, improved passenger experience, and an elevated security baseline. The COVID-19 pandemic in 2020 accelerated TSA's shift to contactless and remote screening, while a continued drive toward IT systems modernization will enable integration, automation, and operational efficiency. A continued focus by international leadership on LPD airports and one-stop security pilots aims to facilitate international travel. In addition, cyber threats have intensified the need to secure aviation and surface systems, along with infrastructure, against cyberattacks.

The investments identified in the CIP 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, 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. TSA therefore 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

A. Vetting and Biometrics

1. Vetting

Vetting Capability Overview: At the Transportation Security Administration (TSA), vetting is defined as the process by which data provided by passengers and credentialed populations (for example, 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.

Vetting is a critical part of identity management (IDM) and works in tandem with identity proofing and identity verification to ensure that TSA enables only the right persons to be granted the right access or a credential based on their biographic and biometric information. 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 A1: Vetting Capability Funding Profile

Vetting Capability - Fiscal Year (FY) 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023–FY 2027 Total**
Vetting & Credentialing System (VCS)	$85.1	$81.6	$78.6	$77.3	$76.1	**$398.7**
Secure Flight	$135.0	$136.0	$136.7	$137.5	$138.3	**$683.5**
Total Vetting Capability	**$220.1**	**$217.6**	**$215.3**	**$214.8**	**$214.4**	**$1,082.2**

FY 2023-FY 2027 reflects the FY 2023 Congressional Justification (CJ).

i. Vetting and Credentialing System

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. VCS 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.

VCS improves our Nation's defense against terrorism by matching biographic data to terrorist-related information. VCS has an overall mission to develop timely, actionable, and valuable information based on automated scoring methodologies, automated and manual intelligence analysis and verification, and vulnerability assessments designed to identify and report individuals with a known or potential terrorist nexus, in order to mitigate risk to the National Transportation Infrastructure.

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 Federal Information Security Management Act (FISMA) system boundaries that include Technology Infrastructure Modernization 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 A2: VCS Funding Profile

Vetting and Credentialing System – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-FY 2027 Total**
Technology Infrastructure Modernization	$23.1	$22.7	$22.5	$22.4	$22.3	$113.0
Vetting Fees	$62.0	$58.9	$56.2	$54.9	$53.8	$285.8
Total VCS	**$85.1**	**$81.6**	**$78.6**	**$77.3**	**$76.1**	**$398.8**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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 credential authentication technology (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 A3: Secure Flight Funding Profile

Secure Flight – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Secure Flight	$132.5	$133.4	$134.2	$134.9	$135.7	$670.8
Traveler Redress Inquiry Program	$2.5	$2.5	$2.6	$2.6	$2.6	$12.8
Total	**$135.0**	**$136.0**	**$136.7**	**$137.5**	**$138.3**	**$683.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

Future of the Vetting Capability: TSA published the strategic IDM Roadmap that outlines goals and objectives for exploring additional research and development (R&D) activities to enhance standards and its risk management framework, to evaluate existing and available data sources, and to explore automation to improve vetting processes. TSA aims to make technological and functional process improvements to increase the speed and accuracy of vetting results and to understand and assess better the risks posed to the transportation system.

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.
- Develop supporting infrastructure for biometric solutions.

IDM at TSA is the continuous process of ensuring that the right people have access to the right transportation areas, 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 & 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 IDM Roadmap. Identity proofing and enrollment is the act of confirming that someone is who he or she claims 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. Moreover, as TSA prepares for full enforcement of REAL ID, it will need to examine technology's potential to provide an alternate means of verifying a person's identity. As TSA implements new proofing solutions, it will need to invest in technologies and tools that support these efforts across various airport touchpoints and populations.

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 checkpoints with the latest technology:

- Biometric technology through enhancements to systems and collection of biometrics to verify identity at the checkpoint;
- R&D to develop the back-end architecture needed 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
- Digital identity solutions that allow digital identities and mobile driver's licenses (mDL) to be accepted at the checkpoint.

Figure A4: IDM Funding Profile

Identity Management – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
CAT	$26.1	$26.1	$26.1	$26.1	$26.1	$130.5
Identity Investment	$3.0	$3.0	$3.1	$3.1	$3.1	$15.3
Boarding Pass Scanner (BPS)	$0.4	$0.3	$0.3	$0.3	$0.3	$1.5
Subtotal Operations and Sustainment	**$29.5**	**$29.4**	**$29.4**	**$29.5**	**$29.5**	**$147.3**
CAT	$0.0	$0.0	$0.0	$0.0	$0.0	$0.0
Subtotal Procurement, Construction, and Improvements (PC&I)	**$0.0**	**$0.0**	**$0.0**	**$0.0**	**$0.0**	**$0.0**
mDL	$4.3	$4.3	$4.3	$4.3	$4.3	$21.3
Subtotal R&D	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$21.3**
Total	**$33.8**	**$33.7**	**$33.7**	**$33.7**	**$33.7**	**$168.6**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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

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 Transportation Security Officers (TSO) to use their training and experience to focus more on anomalies and error resolution. In the current Coronavirus Disease 2019 (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 pilot programs have helped balance technical developments and usability requirements to inform long-term requirements development. The small-scale tests also have 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. Moving forward, TSA

must consider innovative solutions that allow IDM improvements, while mitigating potential risks that these new technologies may introduce to our transportation system. TSA will continue to work to improve user experiences through testing solutions that increase the level of self-service and front-end tools available or when exploring biometric identity verification solutions.

ii. Credential Authentication Technology

Overview: CAT provides the primary means for authenticating identification document (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.

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.

Figure A5: CAT

As of December 3, 2021, the fleet consists of approximately 1,520 CAT systems operating across 166 facilities (airports/training and testing centers). The CAT program reached full operational capability (FOC) with 1,520 units deployed in the first quarter of FY 2022.

Future State: 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 3, 2023. CAT also is evaluating an enhancement called 2-Way Communications. This feedback mechanism allows CAT to return transactional data to Secure Flight for analytical purposes to help to improve data processes and to ensure matching information. Lastly, CAT is entering Phase II of demonstrating a wireless connection in an operational environment.

In addition, the CAT program is re-baselining to increase the FOC quantity and to implement requirements supporting a self-service version of the current CAT system (second generation CAT (CAT-2)), including a camera for 1:1 facial biometric verification, and authentication of mDLs. At current projected funding levels, the CAT program will not achieve the new FOC of 3,585 systems (one per lane) until FY 2048. CAT-2 will be built on the existing CAT infrastructure.

Figure A6: CAT Funding Profile

CAT - FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023 - 2027 Total**
CAT	$26.1	$26.1	$26.1	$26.1	$26.1	$130.5
Total CAT	**$26.1**	**$26.1**	**$26.1**	**$26.1**	**$26.1**	**$130.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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 (for example, young children) and in other limited circumstances.

Figure A7: BPS

Future State: BPSs will continue to be the primary screening system for passengers without identification as a strategy 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 2,850 BPSs are available for use (as of December 2021).

Figure A8: BPS Funding Profile

BPS - FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
BPS	$0.4	$0.3	$0.3	$0.3	$0.3	$1.5
Total	**$0.4**	**$0.3**	**$0.3**	**$0.3**	**$0.3**	**$1.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

Future of the IDM Capability: TSA released the IDM Roadmap, which serves as the standard for new and expanded IDM capabilities. 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. TSA is working to evolve and manage a cohesive IDM ecosystem within TSA and with its partners that improves security effectiveness, the human experience, and operational efficiency for current and pending 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 meet better 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 that TSA is equipped to integrate emerging technology at the TSA checkpoint. Priority investments in IDM capabilities are detailed below:

CAT-2: To achieve the goals laid out in the IDM Roadmap, TSA is upgrading its CAT machines with biometric, digital identity, and self-service capabilities in response to COVID-19 (CAT-2), to the need to accurately identity passengers, and to the growing availability of robust identity solutions in the market. In line with the increased need to shift to more contactless and automated screening, CAT-2 automates existing high-touch actions at the TDC. In 2020, TSA began piloting the new self-service technology, evaluating how CAT-2 performs in an operational environment to refine necessary modifications before final solution development and

deployment to the field. TSA actively is developing the integration of mDL authentication capability with CAT-2 to process digital identity information and to verify a person's identity at the airport checkpoint. TSA is piloting an AutoCAT solution that will automate the CAT-2 technology further by introducing an e-gate form factor for seamless passenger control and will evaluate automating all the TDC functions so that the officer can focus on identity resolution or other priorities.

Facial Identification Solution: The Joint TSA-CBP Policy on the Use of Biometric Technology enabled the execution of a series of biometric technology pilots to automate identity verification at the TSA checkpoint through the integration of TSA and CBP's infrastructure. These pilots focus on testing a facial identification solution that utilizes a back-end repository to compare a live-image capture of consenting eligible travelers to a gallery of enrolled facial reference images at the TDC. To continue this development effort, TSA has begun a pilot to test the use of CBP's Traveler Verification Service at TSA checkpoints with the trusted traveler population (TSA PreCheck® or Global Entry) departing on domestic flights. The pilot leverages the TSA PreCheck® Innovation and Piloting Environment on the Security Threat Assessment Mission Platform General Support System to retrieve the traveler's vetting status from Secure Flight and process match requests and results to and from the Traveler Verification Service. Other pilot efforts will help TSA to develop processes to test requirements for non-checkpoint biometric capabilities owned by third parties.

Digital Identity: State Departments of Motor Vehicles, federal agencies, foreign governments, and even private-sector entities (such as banks, airlines, airports, etc.) are developing a wide and growing variety of mobile digital identity credentials for their citizen or customer use cases. TSA actively has engaged industry and interagency partners to expand the use and integration of digital identity solutions in its transportation arenas to mirror customer expectations (for example, digitization of key services and experiences) in their travel experience. TSA's ability to "trust but verify" digital identities must mature to keep pace with industry and interagency developments. In the future, TSA will help to shape the digital identity market to ensure that aviation security needs are prioritized and met. Through a repeatable, standards-based methodology, TSA will be able to achieve high identity assurance and interoperability with the CAT-2 fleet and future enrollment platforms.

Figure A9: mDL Funding Profile

Mobile Driver's License - FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023 - 2027 Total**
mDL	$4.3	$4.3	$4.3	$4.3	$4.3	$21.3
Subtotal R&D	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$21.3**
Total	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$4.3**	**$21.3**

FY 2023-FY 2027 reflects the FY 2023 CJ.

B. Threat Detection System-Of-Systems

1. Accessible Property Screening

Accessible Property Screening (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.

APS highlights several functional areas that allow TSA both to mature the capability and to meet developmental objectives at security checkpoints nationwide. The APS 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 Checkpoint Property Screening System (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 A10: APS Capability Funding Profile

Accessible Property Screening – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
CPSS O&S	$55.1	$55.9	$56.0	$56.0	$56.1	$279.1
Advanced Technology (AT)	$69.6	$69.7	$69.8	$69.8	$69.9	$348.9
Subtotal O&S	**$124.8**	**$125.6**	**$125.7**	**$125.9**	**$126.0**	**$627.9**
CPSS PC&I	$105.4	$95.9	$95.9	$95.8	$95.7	$488.7
Subtotal PC&I	**$105.4**	**$95.9**	**$95.9**	**$95.8**	**$95.7**	**$488.7**
Total APS	**$230.2**	**$221.5**	**$221.6**	**$221.7**	**$221.7**	**$1,116.7**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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

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 three-dimensional (3D), high-resolution, X-ray images for automated threat recognition algorithms. The deployment of these CT systems provides an enhanced imaging platform for screening carry-on bags and other accessible property at security checkpoints, and enables the detection of a broader range of threats. 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.

TSA began the CPSS Acquisition Program in 2019 to deploy a long-term CT solution incrementally with enhanced threat detection algorithms, ingress/egress, and networking capabilities. The CPSS acquisition strategy allows TSA to deploy an initial capability and to expand functionality incrementally as the program proceeds to FOC and beyond. The primary objective of CPSS is to deploy and integrate effective APS solutions with existing or modified security screening processes and technologies to outpace emerging threats, enhance security efficiency, and improve the passenger experience.

TSA is pursuing and sustaining four CPSS system configurations: AT/CT, CPSS base, CPSS mid-size, and CPSS full-size. Multiple configurations provide flexibility for installation and operations at airport checkpoint facilities with varying sizes, passenger demand volumes, and activity profiles. The CPSS Base systems have the same hardware components (screener assist for explosives and prohibited items, equipped with gravity rollers and manual diverters) and Accessible Property Screening Systems (APSS) 6.2 Level 0 Threat Detection Algorithm as AT/CT, but meet the CPSS requirements and are Security Technology Integrated Program (STIP) Client- compatible. In addition to base capabilities, mid-size systems include ingress and egress conveyors and an operator-initiated auto-diverter allowing TSOs to divert bags with suspicious items to separate conveyors for secondary/manual inspection. In addition to m-size capabilities, full-size systems include an automated bin return, high-threat containment device, and automated conveyance system that allows multiple passengers to divest at the same time.

Because of the enhanced capabilities offered by CT systems, the CPSS Program is conducting a one-for-one replacement of the AT systems with the 3D CT systems. Based on this, the CPSS Program's FOC is 2,263 systems, however, the program may procure beyond this quantity to meet future airport growth and expansion needs. To date, the CPSS Program has deployed 300 AT/CT systems to airports nationwide and deployments are ongoing for the recently purchased 314 mid-size CT systems. At

Figure A11: CT

current projected funding levels, the CPSS program will achieve FOC in FY 2042.

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.

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.

- **CPSS Increment 2 (FY 2024-FY 2027)**: Procure and deploy CPSS configurations with an advanced threat detection standard and STIP connection (networked).

Key Activities:

- TSA completed deployments of the 300 AT/CT systems procured under the AT Program, in April 2021. All the AT/CT systems now have 6.2 Level 0 detection algorithm activated.
- **Increment 1** – In alignment with Increment 1, TSA is working on the following activities.
    - Under the CPSS Program, TSA has completed the qualification process and Qualified Products List approval successfully for three CPSS systems; TSA now has a vendor system representative for each of the configurations (base, mid-size and full-size) on the Qualified Products Lists.
    - TSA awarded the first CPSS mid-size system order to Analogic Corporation for the procurement of 314 mid-size systems and is on track to award the first base and full-size system orders. As of January 31, 2022, 10 mid-size systems have been deployed and deployments are expected to continue through 2022.
- **Increment 2** – In support of Increment 2 and future increments planning, TSA released a request for information for the STIP integration implementation. Based on the responses received from industry, the CPSS Program is working on defining the scope of STIP for Increment 2.
- **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 is piloting certified APSS v6.2 Level 1 algorithms on CT systems in airports; APSS v6.2 Level 2 certification should be completed in the fourth quarter of FY 2023.

- Undergoing field demonstration for **prohibited items algorithms** to expand detection and to minimize false alarms to be piloted at Harry Reid International Airport in the second quarter of FY 2022.

- **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 piloting remote screening/cross-lane screening capabilities at Hartsfield - Jackson Atlanta International Airport, Miami International Airport (MIA), and George Bush Intercontinental Airport to improve utilization of current resources, to determine options for staffing optimization, and to limit passenger contact in light of the COVID-19 pandemic.
- **Open Architecture** – Integration of Digital Imaging and Communications in Security (DICOS) standardized data formats and Open Platform Software Library (OPSL) standardized interfaces to enable more advanced functionality in the long term, including 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.

Figure A12: CPSS Mid-Size

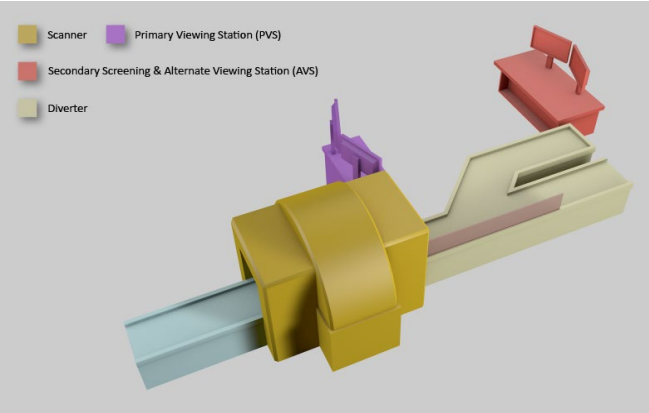


Figure A13: CPSS Full-Size

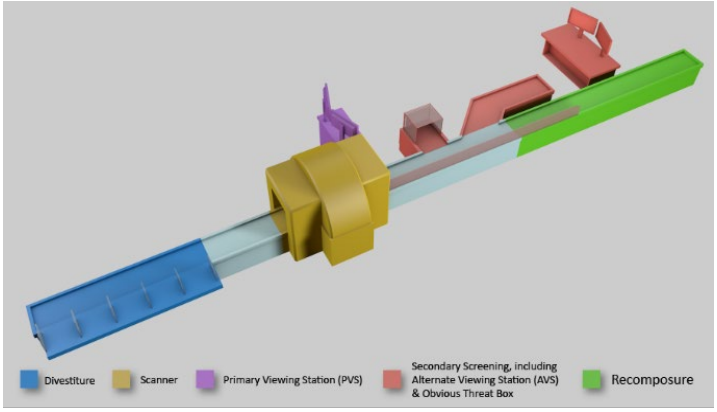


Figure A14: CPSS Funding Profile

CPSS – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
CPSS O&S	$55.1	$55.9	$56.0	$56.0	$56.1	$279.1
CPSS PC&I	$105.4	$95.9	$95.9	$95.8	$95.7	$488.7
Total CPSS	**$160.5**	**$151.8**	**$151.8**	**$151.8**	**$151.8**	**$767.8**

FY 2023-FY 2027 reflects the FY 2023 CJ.

ii. Advanced Technology X-rays

Overview: AT X-ray systems detect threats concealed in passengers' accessible property upon entrance to the screening checkpoint. Automated Screening Lanes (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 partners with airlines and airports to install ASL units at high-traffic security screening checkpoints and to connect them to existing AT2 systems. ASLs are not procured by TSA; however, TSA assumes costs for maintenance of these donated systems after warranties expire.

Figure A15: AT

Future State: TSA is deploying improved threat detection algorithms to the AT and AT/ASL fleets and additional threat detection algorithms are in development and testing. There are approximately 1,955 AT standalone systems deployed to the field and 236 AT systems integrated with ASLs (as of January 31, 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 A16: AT Funding Profile

AT/CT - FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
AT O&S	$69.6	$69.7	$69.8	$69.8	$69.9	$348.9
Total APS	**$69.6**	**$69.7**	**$69.8**	**$69.8**	**$69.9**	**$348.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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 for checkpoint APS, and where possible, use AR countermeasures to detect and identify the alarmed material without requiring further AAR procedures (requiring explosives experts and/or law enforcement) or devices to resolve the alarm fully.

The AR technology capability is divided into two tracks:

- Track 1 – confirmatory[12] technology is intended to provide positive identification of a substance.
- Track 2 – nonconfirmatory technology may require additional screening (physical search, additional TSE utilized, adjudication by an explosives expert or law enforcement) before a security decision can be reached. The current Explosives Trace Detection (ETD) fleet technology is based on ion mobility spectrometry, a Track 2 – nonconfirmatory technology.

Figure A17: AR Capability Funding Profile

Alarm Resolution – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
ETD	$44.7	$44.7	$44.7	$44.8	$44.8	$223.7
Bottled Liquid Scanner (BLS)	$7.1	$6.6	$6.6	$6.6	$6.6	$33.5
Chemical Analysis Device	$0.8	$0.8	$0.8	$0.8	$0.8	$4.1
Subtotal O&S	**$52.7**	**$52.1**	**$52.1**	**$52.2**	**$52.2**	**$261.3**
Emerging AR 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	**$55.7**	**$55.1**	**$55.1**	**$55.2**	**$55.2**	**$276.3**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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

i. Explosives Trace Detection

Overview: The current ETD fleet technology is based on ion mobility spectrometry, a Track 2 technology. ETD is TSA's most-used AR capability. The high sensitivity of ETD systems enables TSOs to perform fast and accurate screening for explosive trace from a wide range of explosive threats on a variety of surfaces. ETD units screen for these quantities on passengers, their accessible property, and checked baggage.

Figure A18: ETD

The ETD fleet consists of approximately 5,835 deployed units; 3,388 in Checkpoint and 2,447 in Checked Baggage areas (as of January 31, 2022) and the program has reached FOC. The ETD program is executing software and hardware component upgrades for fielded systems to address evolving threats. These enhancements, including a 6.2/6.3 detection standard upgrade, will continue as new AR technologies are developed to replace the ETD fleet. Periodic purchases of current ETD system models are focused on airport growth, expansion, and maintaining safety stock levels.

[12] Confirmatory: Ability to identify and analyze the alarm material with no further procedures or TSE required to verify whether the material is benign, and if the alarm can be cleared or if it remains a potential threat that is elevated to AAR explosives experts.

Future State: The current ion mobility spectrometry fleet will continue to support AR as the primary Track 2 – nonconfirmatory technology until the next generation of AR TSE is identified to replace the existing TSE in the ETD fleet.

Figure A19: ETD Funding Profile

ETD – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023 -2027 Total**
ETD	$44.7	$44.7	$44.7	$44.8	$44.8	$223.7
Total ETD	**$44.7**	**$44.7**	**$44.7**	**$44.8**	**$44.8**	**$223.7**

FY 2023-FY 2027 reflects the FY 2023 CJ.

ii. Bottled Liquid Scanner

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 2021) are deployed to the field. BLSs are part of the Passenger Screening Program (PSP) legacy. TSA is procuring BLSs periodically to meet airport growth, expansion, and safety stock needs.

Figure A20: 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.

Figure A21: BLS Funding Profile

BLS – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023 - 2027 Total**
BLS	$7.1	$6.6	$6.6	$6.6	$6.6	$33.5
Total AR	**$7.1**	**$6.6**	**$6.6**	**$6.6**	**$6.6**	**$33.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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. 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:

Figure A22: Emerging Technologies

- 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 A23: Emerging Technologies Funding Profile

Emerging Technologies – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Emerging AR 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	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$3.0**	**$15.0**

FY 2023-FY 2027 reflects the FY 2023 CJ.

Future of the AR Capability: The future of AR is outlined by the TSA AR Roadmap, updated annually, highlighting the technologies, process, and capabilities required to take AR from the current state to the next-generation capability. TSA is investing in deploying next-generation passenger and baggage screening technologies (such as checkpoint CT systems). If the next generation of AR technologies is not developed and deployed in concert with checkpoint CTs, preliminary analysis shows potential for increased "threat loss" at airport checkpoints affecting AR capability to verify all threats identified by primary screening. As a result of this risk, along with the potential negative impact on TSO workload and passenger wait times, TSA will develop and test emerging AR technologies to address a wider range of explosive/chemical/biological/

radiation/nuclear threats, will mitigate complex concealments, and will enhance the overall screening baseline.

AR will look 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, to reduce labor-intensive processes, and to simplify operations, in part by improving procedures and by utilizing new technology that will identify more benign materials, thus resulting in the confiscation of fewer passenger items that commonly are seen in the normal stream-of-commerce and reducing overall passenger wait times that can be linked to cumbersome AR and AAR processes related to known technology capability gaps.

AR also will look to demonstrate new efficiencies enabled by networking, using open architecture 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 Headquarters timely insight to improve screening effectiveness and to lower primary screening false-alarm rates through 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 DICOS 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).
- 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. With funding received in FY 2022, TSA is looking to integrate the low probability of false alarm (Pfa) algorithm developed by Leidos for the AIT-1 to extend the effective lifespan of the current OPS TSE. 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 socially distanced checkpoint.

Figure A24: OPS Capability Funding Profile

On-Person Screening – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
AIT	$55.8	$55.8	$55.8	$55.8	$55.8	$278.9
PSP EMDs	$5.1	$5.8	$5.8	$5.8	$5.8	$28.2
Subtotal O&S	**$60.8**	**$61.5**	**$61.6**	**$61.6**	**$61.6**	**$307.1**
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 OPS	**$65.8**	**$66.5**	**$66.6**	**$66.6**	**$66.6**	**$332.1**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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

i. Advanced Imaging Technology

Overview: AIT systems use millimeter wave technology to detect undivested items on travelers. This OPS technology increases detection capability of metallic and nonmetallic threats, such as explosives, and reduces physical pat-downs at security checkpoints.

Figure A25: 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 seven primary planned milestones between FY 2023 and FY 2027, dependent on availability of funds:

- AIT Windows 10 universal software modernization (FY 2022-FY 2023);
- Post-implementation Review (FY 2022-FY 2024);
- Enhanced algorithm and wideband retrofit of current fleet (FY 2022-FY 2026);
- Next-generation OPS technology development (FY 2022-FY 2024);
- Next-generation OPS technology testing (FY 2024-FY 2026);

- 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 2023 budget.

Currently, the AIT fleet includes ProVision Automatic Target Detection (AIT-1) units and ProVision 2 (AIT-2) units. Although new requirements are pushing AIT to the end of its technical limitations, it will continue to be a key component of passenger screening, and is undergoing development efforts to extend its life.

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:

- Retrofit 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.
- Utilize 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.
- Integrate 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.

- Establish and characterize a post implementation review methodology.
- Explore 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 A26: AIT Funding Profile

AIT – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
AIT (O&S)	$55.8	$55.8	$55.8	$55.8	$55.8	$278.9
On-Person Detection/Next-Gen AIT (R&D)	$5.0	$5.0	$5.0	$5.0	$5.0	$25.0
Total AIT	**$60.8**	**$60.8**	**$60.8**	**$60.8**	**$60.8**	**$303.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

ii. PSP Legacy Enhanced Metal Detector

Figure A27: 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. Approximately 1,390 EMDs are in use (as of December 2021).

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 A28: PSP Legacy EMD Funding Profile

EMD – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
PSP Legacy Walk-Through Metal Detectors	$5.1	$5.8	$5.8	$5.8	$5.8	$28.2
Total EMD	**$5.1**	**$5.8**	**$5.8**	**$5.8**	**$5.8**	**$28.2**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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:

- Complete deployment of enhancement packages for AIT-1 and AIT-2;
- Complete HD-AIT Phase 1, a retrofit of the current AIT fleet with enhanced algorithms;
- Complete HD-AIT Phase 2, a retrofit of the current AIT fleet with wideband technology;
- Conduct R&D for detection-at-range capabilities;
- Conduct R&D for nonmetallic walk-through screening solutions; and
- Conduct R&D for next-generation OPS solutions.

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. Recently, the implementation of a new threat detection algorithm on equipment is expected to improve TSA's ability to detect a wider range of threats while decreasing Pfas. TSA is exploring how to route passengers' baggage according to their risk levels, thus decreasing the amount of bags manually searched. TSA also is examining the use of CT machines for both carry-on and checked baggage at low-volume airports. Furthermore, and in conjunction with CBP and S&T, the Checked Baggage CM is exploring a series of proofs-of-concept, such as the One-Stop Security pilot[13], that will help to determine the feasibility of screening baggage virtually to eliminate TSA's need to rescreen baggage from abroad. TSA also is pursuing other technological solutions that decrease the need for opening bags. Long-term checked baggage aims to leverage open architecture capabilities established under CPSS and AIT programmatic efforts, and to support the integration of DICOS standardized data formats and OPSL standardized interfaces. These efforts will enable more advanced capabilities.

Figure A29: Checked Baggage Capability Funding Profile

Checked Baggage FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Screening Technology Maintenance – Electronic Baggage Screening Program (EBSP) - Investment	$256.9	$257.0	$257.2	$257.4	$257.5	$1,286.0
Subtotal O&S	**$256.9**	**$257.0**	**$257.2**	**$257.4**	**$257.5**	**$1,286.0**
Checked Baggage - EBSP - Investment	$13.9	$0.0	$0.0	$0.0	$0.0	$13.9
Aviation Security Capital Fund - EBSP - Investment (Mandatory)	$250.0	$250.0	$250.0	$250.0	$250.0	$1,250.0
Subtotal PC&I	**$263.9**	**$250.0**	**$250.0**	**$250.0**	**$250.0**	**$1,263.9**
Total Checked Baggage	**$520.8**	**$507.0**	**$507.2**	**$507.4**	**$507.5**	**$2,549.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

TSA is developing the following TSE solutions to evolve the Checked Baggage capability:

i. Electronic Baggage Screening Program

Figure A30: EDS

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 technologies, and entering into other transaction agreements with airports. EBSP conducts these

[13] A pilot program located at foreign last-point-of-departure airports that permits passengers and their accessible property to continue on additional flights or flight segments originating in, and inbound to, the United States without additional security rescreening, and for other purposes.

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 1,657 Explosive Detection Systems (EDS). 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 2,684 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.

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, EBSP is working with the Requirements and Capabilities Analysis CM to develop the Capability Roadmap and to implement technology and infrastructure improvements to support the future vision of Checked Baggage.

Future of the Checked Baggage Capability: To address near- and far-term technology, the Requirements and Capabilities Analysis CM, EBSP Program Manager, S&T, and the Homeland Security Operational Analysis Center conducted a study in 2021. This study informs the evolution of the Checked Baggage mission, the Capability Roadmap, the future of the EBSP, investment planning, and industry focus. Ultimately, the end-state is characterized by an increased ability to detect an expanded set of threat materials at higher detection rates, lower false-alarm rates, and lower lifecycle costs.

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 to maintain adequate security for a growing traveling population, TSA must expand access to R&D investments not only through increases in federally allocated funds, but also through interagency and industry partnerships. For Checked Baggage screening, TSA, in coordination with S&T, is pursuing R&D with the potential to implement enhanced threat detection algorithms on new and existing TSE to improve TSA's ability to detect a wider range of threats while decreasing the Pfas.

Furthermore, TSA will continue to seek enhancements to its EDS to improve the performance and capability of existing Checked Baggage screening systems. CT-based technology also is maturing in EDS capability for future use in checked baggage. Also, TSA seeks to improve ETD technology and to integrate 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. The recent study also noted the possible future-case use of artificial intelligence and machine learning for identifying threats with significant up-front human and financial resource allocation. Overall, TSA will identify 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.

5. Multimodal and Public Area Capabilities

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 A31: MPAC Funding Profile

Multimodal and Public Area Capabilities – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
SST	$7.9	$7.9	$7.9	$7.9	$7.9	$39.5
Air Cargo Security Technology Program	$10.8	$10.9	$10.9	$10.9	$10.9	$54.4
Total MPAC	**$18.8**	**$18.8**	**$18.8**	**$18.8**	**$18.8**	**$94.0**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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);
- EO 13416: Strengthening Surface Transportation Security; and
- The FAA [Federal Aviation Authority] Reauthorization Act of 2018 (P.L. 115-254).

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 Surface Security Technology Catalog. Representation in the Surface Security Technology

Catalog does not indicate endorsement for a technology's capabilities or performance but 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 A32: Detection-at- Range

Figure A33: Undercarriage Screening

Figure A34: Standoff Optical Trace Detection

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.
- 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 A35: SST Funding Profile

Surface Security Technology – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
SST	$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 2023-FY 2027 reflects the FY 2023 CJ.

ii. Air Cargo Security Technology Program

Overview: The MPAC Air Cargo Security Technology Program regulates industry use of screening technologies, and develops capability gaps and requirements in collaboration with industry. Air Cargo evaluates and qualifies technologies that detect explosive threats being transported on aircraft, assesses security solutions for all cargo carriers, maintains a qualified list

of cargo screening technologies, and explores emerging counterterrorism capabilities within the Air Cargo mission space. To achieve this, the Air Cargo Program established the Air Cargo Screening Qualification Test process for qualifying air cargo screening technologies to ensure a uniformly high standard of performance in detecting explosive threats. It also publishes the list of authorized systems on the Air Cargo Screening Technologies List (ACSTL), which serves as TSA's official guide for regulated parties to use when procuring screening devices and associated trace consumables in accordance with TSA approved security programs. Any technology purchased from this list must be utilized in accordance with measures outlined in a screener's Standard Security Program. This list does not apply to devices owned by TSA or devices used in TSA-sponsored tests or test beds, but serves as TSA's official documentation for regulated parties to use when procuring screening devices in accordance with TSA approved Security Programs.

Air Cargo mission areas are directed by the following regulatory requirements:

- P.L. 110-53 (9/11 Act), requiring that all air cargo uploaded on passenger aircraft be screened at a security level equal with that of passenger checked baggage
- 100-percent Air Cargo Screening Requirement, which states that 100 percent of cargo to be loaded on a passenger aircraft in the United States must be screened following TSA-approved processes and procedures.
- July 2021 International Civil Aviation Organization (ICAO) requirement that all outgoing United States cargo must be screened according to an approved security program.

The program also focuses on MPAC's mission to provide security technology recommendations and solutions for air cargo by developing requirements for new security technologies in collaboration with industry.

Future State: The Air Cargo Security Program will continue evaluating next-generation technologies to improve security effectiveness and operational efficiency in the air cargo environment. The current Air Cargo Program test and evaluation pipeline consists of more than 15 devices with new submissions being received on a rolling basis in response to open requests for information. In addition, TSA successfully completed the high-priority EDS field assessment and also is preparing a guide on best practices for operator training, message-handling systems configuration, installation, and commissioning. These efforts are setting the stage for the potential future use of next-generation EDS in air cargo, and increased use is expected by screening facilities that use conveyor systems. These emerging technologies would replace existing capabilities to meet new technical and security standards issued by ICAO that require screening of inbound and outbound international cargo transported by a commercial carrier. TSA also plans to refresh the ETD test bed with next-generation technology capable of detecting new threats in the air cargo security landscape.

Nearly 100 screening technology devices are listed on the technology list, the majority of which are X-ray devices. The air cargo industry is experiencing a significant demand for ETD devices customized to the air cargo screening environment. However, ETD technologies, currently based on ion mobility spectrometry, are slow to meet TSA's new requirements. TSA believes the future success of ETD technologies will lie in mass spectrometry and is working with vendors to qualify this next-generation technology. While fewer regulated entities would benefit

from the high speeds offered by EDS, with cost to benefit enough to warrant the high capital investment costs, TSA has seen an uptick in demand for these technologies as well. Development and investment in passenger aviation screening technologies is being leveraged to demonstrate potential for applicability in the air cargo screening environment. However, both ETDs and EDS involve automated detection, which tends to involve significantly more TSA testing resources before receiving TSA approved and qualified ACSTL status. With only two newly approved ETD and EDS technologies on the ACSTL, it is important to foster competition within the marketplace for these technologies. Competition will ensure that optimum performance is achieved at a reasonable price for user adoption.

Figure A36: Air Cargo Security Technology Program Funding Profile

Air Cargo Security Technology Program – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Air Cargo Security Technology Program	$10.8	$10.9	$10.9	$10.9	$10.9	$54.4
Total Air Cargo Security Technology Program	**$10.8**	**$10.9**	**$10.9**	**$10.9**	**$10.9**	**$54.4**

FY 2023-FY 2027 reflects the FY 2023 CJ.

iii. Airport Infrastructure Protection

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 in the public area, including the airport perimeter. AIP uses a sophisticated combination of cameras and analytics sensors to increase overall operational and situational awareness significantly, including detection of intrusions and other unauthorized events and potential threats. AIP is collaborating with two airports, a CAT X and a CAT I, to help to highlight the vulnerabilities at the perimeter of airports and to secure additional funding for further perimeter protection projects. AIP will collect 2 years of data and will develop a final report based on lessons learned, recommendations for the industry on enhancing perimeter intrusion technologies, and operational benefits to installing such technologies at the perimeter of critical infrastructure.

Other transactional agreements (OTA) are an important tool to meet mission needs with local airport authorities. AIP will continue to look for other avenues and requires additional funding that will be used to address the critical capability gaps in the public areas of airports.

Future State: 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 OTAs to test and analyze perimeter security technologies. As of May 2021, the CAT X airport has begun the installation phase of the project. Once

installation is complete, TSA will collect data for up to 2 years to help highlight the vulnerabilities at the airport perimeter and to provide the industry with lessons learned.

iv. Automated Exit Lanes

Overview: One area that AIP has seen a significant interest in is installing automated exit lane technologies. Airports have recognized the operational efficiencies and cost benefits of automated exit lanes. Approximately 25 percent of federalized airports have automated exit lanes as of September 2021; 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 formed a partnership with Ronald Reagan Washington National Airport in January 2021 and collected data on the airport's vendor selection methodologies. In September and November 2021, TSA collected data on the pre-installation assessment, installation, and pre-deployment assessment phases of automated exit lanes. TSA also collected data on the 15 automated exit lanes installed at smaller hubs and non-hub airports, such as Charlottesville-Albemarle Airport and Eugene Airport, in November 2021. This data will be used to inform airport stakeholders on the operational and security benefits, cost benefit analysis, and lessons learned.

Future State: TSA continues to leverage its existing relationships with industry technical experts and vendors to analyze further the benefits of installing exit lane technologies to safeguard the traveling public. If granted future exit lane funding, TSA will visit additional sites to collect operational data on automated exit lanes installed to test further and to recommend technologies to airport stakeholders.

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.

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.

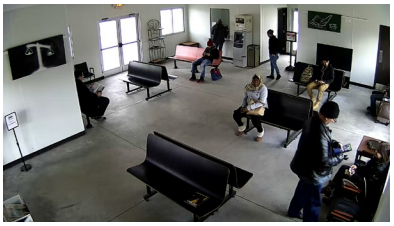


Figure A37: Airport Public Areas

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.

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.

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 biosensing 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:

- 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

Counter-Unmanned Aerial Systems (C-UAS) Capability Overview: The Preventing Emerging Threats Act of 2018[14] gives DHS and the Department of Justice authority to counter threats from unmanned aircraft systems (UAS). This authority allows DHS and the Department of Justice 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. To meet the requirements of the Act, TSA is identifying technology systems that detect, identify, track, and, eventually, mitigate UAS threats in the airport environment. To verify and validate UAS equipment best suited for use in an

[14] https://www.congress.gov/bill/115th-congress/senate-bill/2836#: ~:text=This%20bill%20amends%20the%20Homeland,assets%2C%20through%20a%20risk%2Dbased

airport environment, TSA has established two UAS technology test beds, the first ever at MIA, and a second at Los Angeles International Airport (LAX). These test beds allow TSA to test detection equipment (and eventually C-UAS equipment) to keep up with the rapidly evolving technology marketplace and emerging threats.

TSA's C-UAS capability development is led by the TSA C-UAS Capability Integration Council with the C-UAS Capability Manager as its chair. The Capability Integration Council uses an enterprisewide integration framework, with decision-maker representation from technology requirements and capabilities analysis, operational response and vulnerability assessment, security operations, policy, legal, budget, and IT entities.

The TSA UAS/C-UAS Roadmap aligns with and supports the 2018-2026 TSA Strategy, as well as with ongoing C-UAS efforts identified in Administrator's Intent 2.0 (released in 2020). The roadmap is the strategic planning guide for TSA's efforts that support UAS integration into National Airspace System and C-UAS efforts to protect against threats in the airport environment. TSA anticipates publishing the final roadmap and accompanying fact sheets on cybersecurity, tabletop exercises, and UAS technology testing and evaluation in mid-2022; with an accompanying implementation plan to follow.

TSA co-chairs the C-UAS Technology Working Group, comprised of more than 30 agencies, that reports to the UAS Security Senior Steering Group and UAS Executive Committee. This group facilitates information and resource sharing across the interagency—including technology testing and evaluation results, best practices, and lessons learned—to help to establish standards, to align C-UAS efforts, and to develop C-UAS capabilities.

Deputies from 15 U.S. Government departments and agencies developed and approved the Unified National Level Response to Persistent UAS Disruption of Operations at Core 30 Airports Concept of Operations[15] in October 2019, which was renewed for 1 year effective January 2021, and the process to renew it again is underway. This document designates TSA as the lead federal agency (LFA) for leading a unified national-level response to a persistent UAS disruption at a Core 30 airport. As LFA, TSA implemented a C-UAS assessment unit to complete the training necessary to perform this responsibility, as well as to conduct UAS-specific vulnerability assessments at airports.

TSA is monitoring UAS detections from numbers of sources and integrating the data into a Requirements and Capabilities Analysis Tool that geospatially organizes historical and NRT UAS activity nationwide, helping to increase TSA's air domain awareness and to inform resource allocation prioritization.

[15] The Core 30 Airports are major United States airports as defined by the FAA, available at https://aspmhelp.faa.gov/index.php/Core_30.html

TSA collaborated with its interagency partners, including FAA and DHS S&T, to establish the first-ever operational UAS test bed for UAS detect, track, and identify (DTI) technology at MIA. Additional airports are a high-priority item for DHS and Congress, and test beds will be established as additional resources are provided, with the next test bed established at LAX, and testing to begin in 2022. These operational test beds will allow TSA to continue to deploy, test, and evaluate selected DTI systems to understand better the capabilities and limitations of UAS DTI technologies in an airport environment. TSA is preparing to share technology testing results, best practices, and lesson learned with appropriate interagency stakeholders so that they also may benefit from the information gleaned at the test beds.

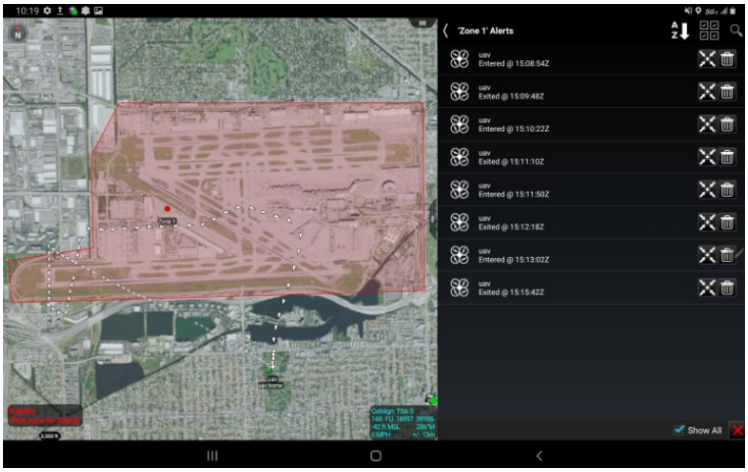


Figure A38: C-UAS Vulnerability Assessment

In addition to DTI systems, TSA plans to evaluate C-UAS mitigation technologies in an operational test bed environment in the future, pending additional authorities from Congress. As TSA is the LFA for response to a persistent UAS disruption at a Core 30 Airport, identifying and evaluating C-UAS technologies will be critical for TSA to meet its LFA responsibilities.

Future State: As the designated LFA for responding to persistent UAS-related incidents at airports, TSA must remain ahead of the adversary by understanding threats, vulnerabilities, and potential countermeasure systems clearly. The number of encounters with UAS around airports and with civil aircraft has increased over the years as UASs proliferate.

TSA completed its Windtalker DTI technology installation at MIA. MIA will begin system configuration to the airport's unique environment before data is collected. TSA also is coordinating with LAX and other stakeholders to continue the establishment of the test bed and plans to begin technology testing in FY 2022.

The capabilities of UASs continue to advance rapidly—they fly longer, faster, with heavier payloads, across farther distances, and more independently—and 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. Without centralized federal guidance, this potentially poses more danger at airports and results in operational and procurement inefficiencies with the deployment of disparate and uncoordinated systems.

Figure A39: C-UAS Funding Profile

Counter-Unmanned Aerial Systems – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Aviation Screening Operations	$5.9	$5.9	$5.9	$5.9	$5.9	$29.7
Mission Support	$1.6	$1.6	$1.6	$1.6	$1.6	$8.1
Other Operations and Enforcement	$3.6	$3.6	$3.6	$3.6	$3.6	$18.2
Subtotal O&S	**$11.2**	**$11.2**	**$11.2**	**$11.2**	**$11.2**	**$56.0**
Total C-UAS	**$11.2**	**$11.2**	**$11.2**	**$11.2**	**$11.2**	**$56.0**

FY 2023-FY 2027 reflects the FY 2023 CJ.

7. National Explosives Detection Canine Team Program

Overview: The National Explosives Detection Canine Team Program (NEDCTP) is a congressionally mandated program[16] that allocates 1,097 Explosives Detection Canine (EDC) teams to the aviation, rail, maritime, and mass transit transportation systems. TSA uses 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 being LEO-led. Of those 675 LEO-led teams, 169 are 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 analytical instruments, a well-trained and supported EDC is the most used and effective detector of explosives.

TSA uses 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 provides 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.

[16] 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).

Over the years, 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 mandated congressionally 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.

Through NEDCTP, TSA will continue to collaborate with federal, state, and local LEAs to expand TSA and LEO participation in explosives detection and deterrence across all modes of transportation. TSA provides state and local LEAs 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.

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.

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

Figure A40: NEDCTP

canine security plan to detect and deter explosive threats better from entering into the aviation, mass transit, rail, maritime, and cargo environments.

Figure A41: NEDCTP Funding Profile

NEDCTP – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
NEDCTP	$140.1	$142.2	$144.0	$145.9	$147.7	$720.0
Canines - K-9 System - Investment	$2.7	$2.7	$2.7	$2.7	$2.7	$13.4
3PK9-C Program	$1.7	$1.8	$1.8	$1.8	$1.8	$8.8
Subtotal Canines without State & Local Law Enforcement	**$144.5**	**$146.7**	**$148.5**	**$150.3**	**$152.2**	**$742.2**
State and Local Law Enforcement EDC Teams	$35.6	$35.6	$35.6	$35.6	$35.6	$177.8
Total Canines	**$180.0**	**$182.2**	**$184.0**	**$185.9**	**$187.8**	**$919.9**

FY 2023-FY 2027 reflects the FY 2023 CJ.

C. Enhanced and Secure IT Systems

1. Information Technology Infrastructure Program

Overview: The secure, reliable IT and communications products, services, and solutions provided by the Information Technology Infrastructure Program (ITIP) 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 32 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 assure uninterrupted operational availability of IT services 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 prioritizes network updates and upgrades through standard annual refreshes of hardware, allowing for the retirement or updating of outdated hardware on a regular basis. Regularly scheduled renewals of this outdated/end-of-life IT infrastructure hardware (servers, network equipment, firewalls) within all datacenter environments and across TSA field sites is critical to address ever-evolving cyber security vulnerabilities, data latency, high-failure rates, sporadic functionality, and high-repair costs. Hardware that is used beyond its manufacturers' end-of-life runs the risk of being overburdened and incapable of sustaining the abundance of new applications that are being developed and performing optimally in an accelerated, agile IT environment. Additionally, end-of-life equipment that no longer receives vendor security patches will increase the risk of cyber threats.

ITIP also is committed to providing TSA users with innovative IT solutions. The Flexible Agile Scalable Teams (FAST) procurement established an IT contract vehicle that supports agile design, development, and application production requirements for a suite of applications that are aligned across the entire agency. Immediate benefits of this procurement type include the flexibility to address all application development requirements and TSA offices, and reducing the acquisition timeline from 6 months to 4 weeks. FAST task orders are designed to support the integration, customization, and development of various mission support systems and applications. They provide full-service, enterprise-focused applications and development capabilities, with IT services delivered through state-of-the-art software systems and dynamic computing environments. The business drivers for the FAST strategy include leveraging industry and government best practices, reducing time-to-market, improving code quality, and enhancing customer service.

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 cloud infrastructure. TSA Azure is continuing the transformation of ITIP through the identification and support of refactoring, or re-writing, applications from on-premises to the cloud environment. TSA Azure 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:** ITIP will continue to build on Defense in Depth, which constitutes a series of defensive mechanisms that are layered in order to protect valuable data and information through: development and enforcement of security policy aligned to mission

objectives, shared cyber-risk ownership and management, and proactive and innovative solutions. Additionally, ITIP will expand protective capabilities, tools, and services while improving the sharing of cyber threat indicators, defensive measures, and other cybersecurity information using reporting and dashboards. 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 is advancing the move 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, providing an ecosystem of cloud targets to support the modernization of TSA's infrastructure and the continued onboarding of applications. The adoption of cloud solutions/services, such as integrations between the current on-premises enterprise to infrastructure-as-a-service, platform-as-a-service, and software-as-a-service, 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. By building a culture of experimentation and innovation using these tools, TSA can prototype and operationalize capabilities rapidly. 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.
- **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.
- **User Experience:** ITIP will continue the delivery of applications by providing information that is easily applicable to the user. In addition, ITIP will emphasize data management and business intelligence capability enhancements to enable users to make data-driven decisions.

Figure A42: ITIP Funding Profile

IT Infrastructure Program – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
ITIP	$385.2	$388.3	$389.6	$394.7	$391.3	$1,949.1
Total ITIP	**$385.2**	**$388.3**	**$389.6**	**$394.7**	**$391.3**	**$1,949.1**

FY 2023-FY 2027 reflects the FY 2023 CJ.

2. Field Information Systems

Field Information Systems (FIS) Capability Overview: The FIS Capability Management team is working with stakeholders to identify the current lifecycle state of systems and customer needs. This will drive the development and update of requirements and specification of a broader integrated view of the FIS capability gaps for TSA. FIS has categorized the capabilities into four areas: Asset Management, Mission Management, Operations Support, and Personnel Management. There currently are more than 32 systems at various timelines in the system lifecycle of innovation, modernization, and O&M.

As the integrated capability and risk analysis subject matter experts, the FIS CM is collaborating with stakeholders to define functional needs and road maps for courses of action. Working with stakeholders, FIS is working to set priorities and to manage a portfolio mix that includes adaptive maintenance work streams for legacy systems, modernization to support process efficiencies and information sharing, and innovation to introduce new capabilities.

Figure A43: FIS Capability Funding Profile

Field Information Systems – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
STIP	$14.3	$14.3	$14.3	$14.3	$14.3	$71.5
Mission & Scheduling Notification System (MSNS) Modernization and Legacy System O&M	$17.5	$17.5	$17.5	$17.5	$17.6	$87.6
Total FIS	**$31.8**	**$31.8**	**$31.8**	**$31.9**	**$31.9**	**$159.2**

FY 2023-FY 2027 reflects the FY 2023 CJ.

Investments within FIS include:

i. Security Technology Integrated Program

Overview: 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: 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 A44: STIP Funding Profile

STIP – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
STIP	$14.3	$14.3	$14.3	$14.3	$14.3	$71.5
Total STIP	**$14.3**	**$14.3**	**$14.3**	**$14.3**	**$14.3**	**$71.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

ii. Mission & Scheduling Notification System Modernization

Overview: MSNS facilitates coordination of air marshal availability and communication of mission assignments with the Federal Air Marshal Service (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.

Figure A45: MSNS Funding Profile

MSNS – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
MSNS Modernization and Legacy System O&M	$17.5	$17.5	$17.5	$17.5	$17.6	$87.6
Total MSNS Modernization	**$17.5**	**$17.5**	**$17.5**	**$17.5**	**$17.6**	**$87.6**

FY 2023-FY 2027 reflects the FY 2023 CJ.

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 law enforcement/FAMS.

Major investment priorities and R&D include stronger enabling systems and processes for screening performance and improved passenger experience; improving officer safety, information processing, and sharing by leaning forward advances in emerging technologies; creating a more connected, interoperable systems architecture; and unlocking cost efficiencies with efficient processes and information systems. FIS CM has identified the following priorities for investment:

- Advancing the Aviation Security Architecture with formal governance processes and integrated information across capabilities;
- Prototyping and deploying Checkpoint Information Management;
- Modernizing and innovating use of field data of transportation security devices, device management, and FISs;
- Advancing field operations schedule management capabilities for security operations and law enforcement/FAMS; and
- Countering the insider threat.

3. Enterprise Physical Access Control System

Overview: The Enterprise Physical Access Control System (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.

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 500 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 March 2022, 52 locations have migrated to ePACS, and 61 TSA locations are planned for migration in FY 2022 and FY 2023.

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 A47: ePACS Funding Profile

Enterprise Physical Access Control System – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
ePACS	$14.5	$14.5	$14.5	$14.6	$14.6	$72.7
Total ePACS	**$14.5**	**$14.5**	**$14.5**	**$14.6**	**$14.6**	**$72.7**

FY 2023-FY 2027 reflects the FY 2023 CJ.

4. Human Capital 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. Specifically, the strategy upgrades the current 13-year-old systems into a more secure, low-risk, and cost-effective, high-productivity environment. The modernization will maximize efficiency through the use of software-as-a-service, robotic process automation, and machine-learning.

By FY 2023, PFP expects leveraged technologies to show trends of realized operational efficiencies. Employee/Manager Self-Service and artificial intelligence automation will improve quality and will reduce times to process candidate forms and personnel transactions. HC modernization will continue to support an innovative workforce through the Candidate Portal, providing live updates of application status; 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; 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 Resources training and business process and systems will continue undergoing a modernization effort to update outdated legacy systems and will 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 2021 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 A48: HC IT Modernization Funding Profile

HC IT Modernization Personnel Futures Program – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
PFP - Mission Support	$134.9	$131.1	$120.7	$119.6	$119.6	$625.9
Screener Training and Other - Personnel Futures - Investment	$13.9	$13.9	$13.9	$13.9	$13.9	$69.3
Total Personnel Futures Program	**$148.7**	**$145.0**	**$134.5**	**$133.5**	**$133.5**	**$695.2**

FY 2023-FY 2027 reflects the FY 2023 CJ.

5. Staffing, Scheduling, Time, and Attendance System

Overview: The Staffing, Scheduling, Time, and Attendance (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 shifts, 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. The application permits TSOs to bid remotely on both annual leave and shifts, per Collective Bargaining Agreement guidelines. Currently, Scheduling, Management, and Resource Tasking is working to integrate with another scheduling software to streamline self-service leave requests.
- Enhanced Staffing Model 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 use TSA's existing website management tools to provide an effective and quick path to production capability. SSTA will integrate the following systems: Advanced Scheduling Tool, eTAS, the Enhanced Staffing Model, and Plan of Day 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, and will increase visibility and management of resources and operations at airports.

The Plan of Day will be used to determine short-term staffing needs (0-2 days), to improve workforce utilization, and to inform operational decisions throughout the course of the day. Optimized operational scheduled data then will be shared with the Kronos system to simplify

time and attendance management. SSTA will provide automation and integration across the enterprise. Greater integration and automation of subsystems will enable optimization of the current TSA field staff at airports nationwide. This will reduce the number of officers removed from their primary job functions as defined by their job analysis tool to assist with administrative duties. SSTA is focused on supporting airport operations and the Administrator's initiative of returning TSOs to the checkpoints. TSA envisions SSTA as a hybrid cloud solution that will assist TSOs in performing time, attendance, scheduling, and budget functions at federalized airports.

Figure A49: SSTA Funding Profile

SSTA System – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
eTAS - Investment	$3.7	$3.7	$3.7	$3.7	$3.7	$18.5
SSTA - Mission Support - Enterprise Services	$8.2	$8.2	$8.2	$8.2	$8.2	$41.0
Total SSTA System	**$11.9**	**$11.9**	**$11.9**	**$11.9**	**$11.9**	**$59.5**

FY 2023-FY 2027 reflects the FY 2023 CJ.

6. Air Cargo IT Systems

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

TSA engages with industry stakeholders to develop IT and data solutions in support of the implementation of TSA's Air Cargo Program. TSA manages 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 managed by the Air Cargo Division within the Policy, Plans, and Engagement Office are supported and implemented through the ongoing development of these systems.

The Air Cargo Management System (ACMS) activities align with TSA leadership goals captured in the Administrator's Intent 2.0 Strategic Goal 1, Improve Security and Safeguard the Transportation System, and in the Air Cargo Security Roadmap under Goal 4, Modernize Air Cargo Policy.

Future State: Currently, the ACMS Branch 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 more than 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.

Although Air Cargo IT Systems are operating a flat funding profile that supports O&M, TSA will identify efficiencies within the program's steady state budget for future modernization efforts. In addition, the Known Shipper vetting contract continues to be funded at $9 million annually. This funding supports the Air Cargo IT program, but is budgeted outside of the Air Cargo IT Systems funding profile.

Figure A50: Air Cargo IT Systems Funding Profile

Air Cargo IT Systems – FY 2023-FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
Air Cargo Security Portfolio - Investment	$13.2	$13.2	$13.2	$13.2	$13.2	$66.0
Total Air Cargo IT Systems	**$13.2**	**$13.2**	**$13.2**	**$13.2**	**$13.2**	**$66.0**

FY 2023-FY 2027 reflects the FY 2023 CJ.

II. TSE Acquisition Update

This section compares security-related technology (SRT) acquired against the planned technology programs and projects.

TSA operates legacy equipment while evaluating potential replacements in an affordable manner. One way to increase affordability and to decrease complete system replacements is the procurement and deployment of technologies to upgrade existing machines as new capabilities arise. TSA takes an incremental approach in developing and deploying enhanced threat detection performance and AR capabilities. When upgrades are not possible to avoid obsolescence, recapitalization remains the sole solution.

The following acquisitions include TSA projections:

- **CAT Units in FY 2021:** The program completed the deployments of 1,520 systems at 119 facilities, including airports, the Federal Law Enforcement Training Center, and the TSA System Integration Facility, on December 29, 2021, reaching current program FOC. The Program Management Office intends to increase the current FOC up to 3,582 units as part of a re-baseline, which TSA plans to achieve by the fourth quarter of FY 2024.

- **CT Units in FY 2021:** TSA deployed 300 AT/CT systems with APSS 6.2 Level 0 detection algorithm to high-risk airports, and procured 314 CPSS mid-sized systems. The AT/CT project enabled high-priority airports to have operational CT capabilities in FY 2021 and allows the CPSS Program to actively incorporate AT/CT project lessons learned into program planning and execution.

- **EDS Units in FY 2021:** TSA installed 52 of the 100 units procured in late FY 2019 to support recapitalization efforts and deployment of new inline checked baggage screening systems. Procurement quantities are based on airport equipment requirements and depend on the timelines for project execution at each specific airport site.

- **AIT Units:** In late FY 2019, TSA procured 100 AIT units and as of October 27, 2021, all 100 units have been installed.

III. PSP Legacy Program Funding Profile

The PSP Legacy program contains four technologies (BLS, BPS, Chemical Analysis Device, and Walk-Through Metal Detectors). 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 A51: PSP Legacy Funding Profile

Passenger Screening Program Legacy – FY 2023 - FY 2027 ($ in millions)						
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2023-2027 Total**
BPS	$0.4	$0.3	$0.3	$0.3	$0.3	$1.5
BLS	$7.1	$6.6	$6.6	$6.6	$6.6	$33.5
Walk-Through Metal Detectors	$5.1	$5.8	$5.8	$5.8	$5.8	$28.2
Chemical Analysis Device	$0.8	$0.8	$0.8	$0.8	$0.8	$4.1
PSP Legacy Pay	$2.0	$2.0	$2.0	$2.1	$2.1	$10.2
Total PSP Legacy	**$15.5**	**$15.4**	**$15.5**	**$15.5**	**$15.5**	**$77.4**

FY 2023-FY 2027 reflects the FY 2023 CJ.

IV. 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),[17] 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

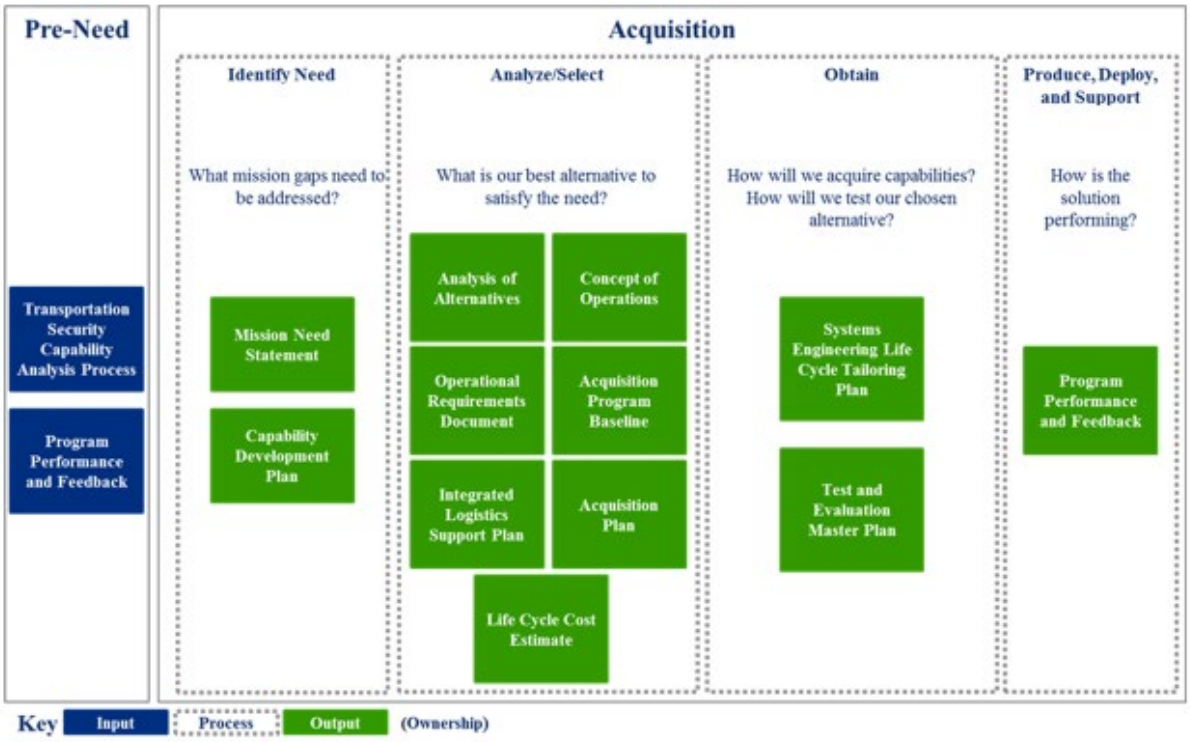
Aligning Resources in Pre-Need

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.

The chart below shows the subsequent phases of the lifecycle that TSA will execute to acquire a material solution.

[17] 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 A52: Overview of the Acquisition Lifecycle for 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.

V. 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 2022 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 A53: 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.

Requirement	Requirement Description	Report Location
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
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

Requirement	Requirement Description	Report Location
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
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

Requirement	Requirement Description	Report Location
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
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*

Requirement	Requirement Description	Report Location
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
(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

Requirement	Requirement Description	Report Location
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

VI. Abbreviations

Abbreviation	Definition
3D	Three-Dimensional
3PK9-C	Third-Party Canine Cargo Screening
AAR	Advanced Alarm Resolution
AR	Alarm Resolution
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
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
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
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
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
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
O&M	Operations and Maintenance
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
R&D	Research and Development
RTSPA	Risk and Tradespace Portfolio Analysis
S&T	DHS Science and Technology Directorate
SRT	Security-Related Technology
SST	Surface Security Technology
SSTA	Staffing, Scheduling, Time, and Attendance
STIP	Security Technology Integration Program
STSTAC	Surface Transportation Security Advisory Committee
TDC	Travel Document Checker
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
TSSRA	Transportation Sector Security Risk Assessment
UAS	Unmanned Aerial System
VCS	Vetting and Credentialing System