# Capital Investment Plan

FY 2021–FY 2025

*June 30, 2020*

Fiscal Year 2020 Report to Congress

Homeland Security

*Transportation Security Administration*

# Message from the Administrator

June 30, 2020

I am pleased to present the following "Capital Investment Plan" (CIP) for Fiscal Year (FY) 2021–FY 2025, which was prepared by the Transportation Security Administration (TSA).

The report was compiled pursuant to reporting requirements in section 223 of the FY 2020 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-93), as well as in the accompanying Joint Explanatory Statement and House Report 116-180, 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 replacement of aged, transportation security equipment (TSE).

TSA partners with other DHS Components including the Science and Technology Directorate (S&T), with the Transportation Security Lab, and with industry partners in aviation and surface to place technology in the hands of our men and women to enhance significantly our security capability.

As TSA's risk landscape evolves, it must continue to invest in acquiring and fielding new technologies to strengthen transportation security. The CIP provides a cohesive view of the 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 its critical mission.

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

The Honorable Nita M. Lowey
Chairman, House Committee on Appropriations

The Honorable Kay Granger
Ranking Member, House Committee on Appropriations

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

The Honorable Patrick J. Leahy
Ranking Member, Senate Committee on Appropriations

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

The Honorable Mike Rogers
Ranking Member, House Committee on Homeland Security

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

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

I appreciate the opportunity to combine our previous reporting requirements to provide a more comprehensive description of TSA's capital investment plans. If I may be of further assistance, please do not hesitate to contact me at (571) 227-2801.

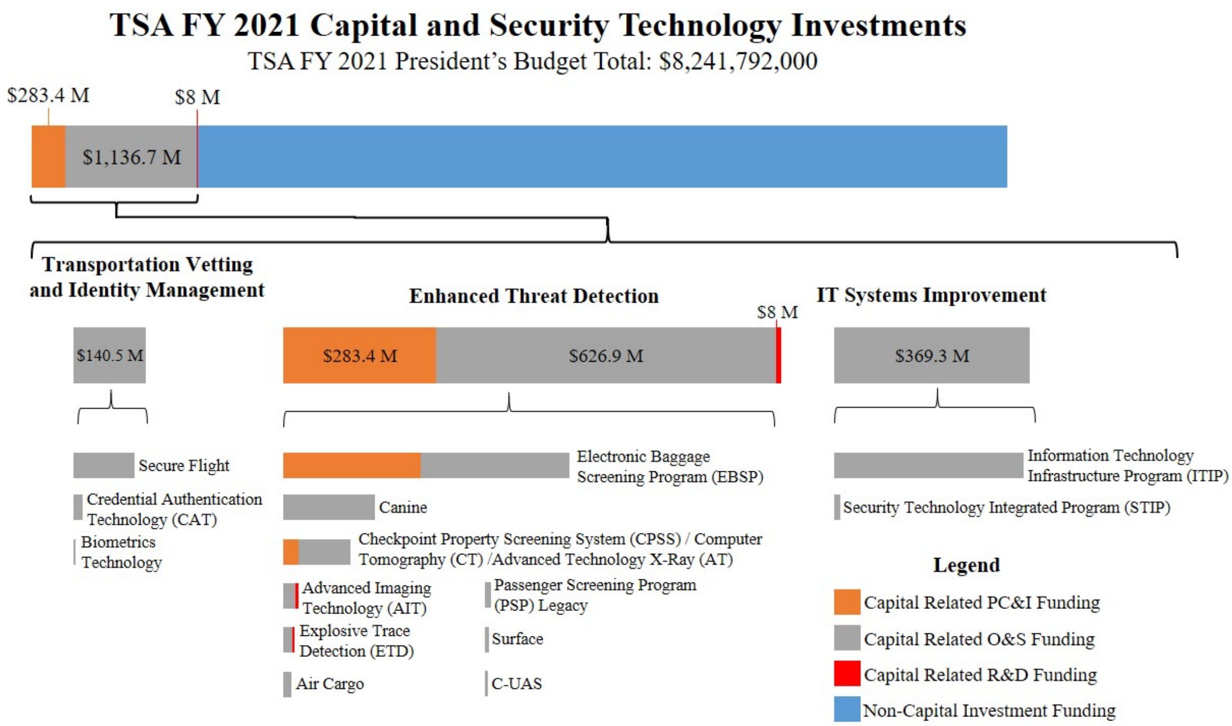
Sincerely,

David P. Pekoske
Administrator

# Executive Summary

The TSA CIP for FY 2021–FY 2025 outlines TSA's strategy for continuous and sustained investment in new, and the replacement of aged, TSE. This submission demonstrates how TSA continues to move toward its strategic priorities within its resource constraints given the increasing demands and dynamic threats facing full transportation security. TSA must continue to invest in acquiring and fielding new technologies to strengthen transportation security. Figure 1 shows the percentage 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 continues to evolve, and passenger and cargo volumes expand, TSA must continue to invest in acquiring and fielding new, sustainable solutions that strengthen the security of the transportation system, while also enhancing the passenger experience and supporting the movement of commerce. The CIP covers the next 5 fiscal years' planned expenditures, based on the Future Years Homeland Security Plan's (FYHSP) authorized levels. Throughout a given fiscal year and over time, requirements may be reprioritized on the basis of changes in the threat environment, operational needs, programmatic reviews, leadership priorities, or other circumstances. Resource levels in the FYHSP do not preclude changes through the annual budget process.

This document provides a cohesive review of the capital investments required to achieve TSA's strategic priorities, to respond to increased passenger demands, and to address the complex challenges of the future within the FYHSP. Figure 3 outlines TSA's FY 2021 budget request.

***Figure 3: TSA Budget Request FY 2021***

| TSA Budget Request FY 2021 (Dollars in Thousands) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 2019 Enacted | | 2020 Enacted | | 2021 President's Budget | | 2020 - 2021 Total Changes | |
| | FTE | $000 | FTE | $000 | FTE | $000 | FTE | $000 |
| Operations and Support | 55,341 | $4,740,079 | 56,159 | $4,850,565 | 54,963 | $4,030,756 | (1,196) | ($819,809) |
| Procurement, Construction, and Improvements | - | $169,789 | - | $110,100 | - | $33,385 | - | ($76,715) |
| Research and Development | - | $20,594 | - | $22,902 | - | $29,524 | - | $6,622 |
| **Net Discretionary** | **55,341** | **$4,930,462** | **56,159** | **$4,983,567** | **54,963** | **$4,093,665** | **(1,196)** | **($889,902)** |
| Offsetting Collections | 249 | $2,904,685 | 249 | $3,061,714 | 332 | $3,892,627 | 83 | $830,913 |
| **Gross Discretionary** | **55,590** | **$7,835,147** | **56,408** | **$8,045,281** | **55,295** | **$7,986,292** | **(1,113)** | **($58,989)** |
| Operations and Support | 17 | $5,200 | 17 | $5,200 | 19 | $5,500 | 2 | $300 |
| Procurement, Construction, and Improvements | - | $250,000 | - | $250,000 | - | $250,000 | - | - |
| **Total Mandatory/Fees** | **17** | **$255,200** | **17** | **$255,200** | **19** | **$255,500** | **2** | **$300** |
| **Total Budget Authority** | **55,607** | **$8,090,347** | **56,425** | **$8,300,481** | **55,314** | **$8,241,792** | **(1,111)** | **($58,689)** |
| Less: Rescissions to Prior Year Balances | - | ($36,544) | - | ($48,143) | - | - | - | $48,143 |
| **Total** | **55,607** | **$8,053,803** | **56,425** | **$8,252,338** | **55,314** | **$8,241,792** | **(1,111)** | **($10,546)** |

# Strategic Alignment

TSA has set ambitious goals over the coming years, striving to improve security and to safeguard the transportation system, to accelerate action, and to commit to its people. To ensure that TSA is well-positioned to act upon this strategy and to modernize and sustain its operations, TSA considers the current and projected outyear transportation environment, including both downside and upside risks and disruptors.

To achieve this strategic vision, TSA categorizes its capital investment in the following three pillars:

- Transportation vetting and identity management
- Enhanced threat detection
- Information technology (IT) systems improvement

**Transportation Vetting and Identity Management:** Investment in the vetting of passengers and credential holders is critical to TSA's ability to identify and mitigate potential security risks.

For instance, deploying Credential Authentication Technology (CAT) will allow TSA to authenticate the security features present on passenger identification documents and to verify vetting status against TSA systems in near real-time so that the passenger receives the appropriate screening based on TSA's assessed risk. Additionally, in 2018, TSA's 2018 "Biometrics Roadmap for Aviation Security and the Passenger Experience" established plans for the use of biometrics to improve both security and the passenger experience. Automating and strengthening current vetting and screening processes through biometrics technology will enable TSA to validate passenger identity for passengers and credential applicants/holders more effectively and efficiently, leading to more accurate assessments of risk.

**Enhanced Threat Detection:** TSA must invest heavily in primary and secondary screening of people and property across the transportation infrastructure to thwart adversaries who constantly seek and develop new explosive materials, weapons, concealment methods, and other tactical and operational approaches. Because aging detection capabilities may not detect and counter these evolving threats effectively, TSA must invest in new technologies and processes to strengthen its security posture.

For example, the deployment of computed tomography (CT) systems for screening carry-on bags and accessible property at the screening checkpoint offers an enhanced imaging platform compared to legacy advanced technology X-rays (AT), and can detect a broader range of threats. Similarly, enhancements in the Explosive Trace Detection (ETD) program will provide TSA with the ability to detect a wider range of explosive threats and to resolve alarms, and investments in next-generation advanced imaging technology (AIT) will improve detection capability and will reduce the necessity of physical patdowns at checkpoints.

**IT Systems Improvement:** In an increasingly connected technology landscape, investments in IT and communication technology are highly interdependent on investments in adjacent technologies. TSA's current system has limited capabilities to transfer and standardize information rapidly in support of operational decision-making. Capital investment in the Information Technology Infrastructure Program (ITIP) will provide modern IT services to enhance TSA's ability to collect, process, and analyze data, and to transfer voice, video, or digital information. Additionally, the Security Technology Integration Program (STIP) will connect TSE to a single network and enable enhanced security effectiveness, information sharing, and data management and analyses.

TSA is charged with securing the Nation's transportation systems from all threats, including cyber and physical attacks. To meet the burgeoning cybersecurity threat environment and expanding intermodal requirements, TSA will invest capital funding in enhanced cybersecurity capabilities to identify risks, to reduce vulnerabilities to systems and critical infrastructure, to mitigate consequences when incidents occur, and to ensure the resiliency of the transportation system.

## The Need for Investment

TSA must identify and align resources to its mission needs in order to maintain adequate security for a growing traveling population. Although TSA continues to achieve its national security

mission within the limits of its current budget authority, funding demands of current operations make it increasingly difficult for TSA to allocate adequate resources to ensure future capability investment.

**Capital Investment:** Continuous and sustained capital investment is necessary for TSA to achieve its mission, but is currently only a fraction of TSA's overall budget authority. Without appropriate capital investment funding, TSA must narrow its focus to programs, rather than take a holistic approach to meeting national security mission needs. Despite a relatively flat topline, the FY 2021 TSA budget request includes funds for investment programs to maintain, purchase, and deploy a minimal number of next-generation TSE; to address retention for transportation security personnel; to continue building a cybersecurity workforce; and to support increasing maintenance costs.

**Research and Development (R&D):** TSA's mission success depends on robust and coordinated investment in capital assets and applied research, development, test, and evaluation activities to advance innovative technology solutions and to support TSA's security infrastructure. TSA continues to benefit from partnerships with other Federal Government departments and agencies such as S&T, the U.S. Department of Energy, the U.S. Department of Defense, and the U.S. Department of Justice. TSA coordinates R&D activities across these organizations and private industry to ensure that efforts are not duplicative and that they support the successful transition of technologies and solutions to operations. In FY 2021, TSA has requested $29,524,000 in R&D funds. The planned distribution of those funds is shown in Figure 4.

***Figure 4: R&D Investment FY 2021 (as of February 2020)***

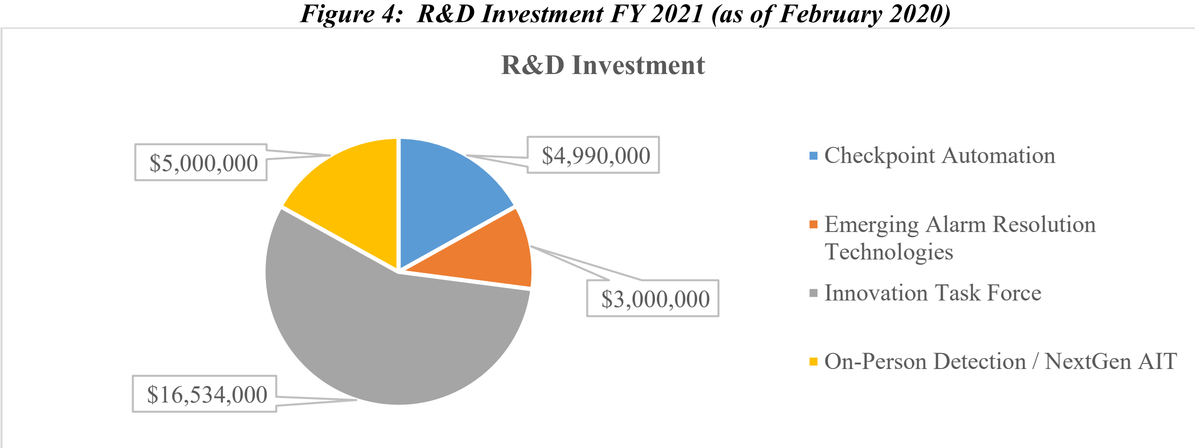


Figure 5 shows a summary of all capital investments discussed in detail in this document.

***Figure 5: CIP Summary Table FY 2021–FY 2025[1]***

| CIP –FY 2021–FY 2025 ($M) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Program** | **FY 2019 Enacted** | **FY 2020 Enacted** | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** | **FY 2021-2025 Total** |
| **Transportation Vetting & Identity Management** | **$132.4** | **$133.9** | **$140.5** | **$133.6** | **$116.9** | **$117.4** | **$119.4** | **$627.7** |
| **Secure Flight** | $113.9 | $115.7 | $117.9 | $121.6 | $106.5 | $107.6 | $109.3 | $562.9 |
| **CAT** | $18.5 | $18.3 | $20.6 | $10.0 | $5.4 | $4.7 | $5.1 | $45.8 |
| **Biometrics Technology** | $0.0 | $0.0 | $2.0 | $2.0 | $5.0 | $5.0 | $5.0 | $19.0 |
| **Enhanced Threat Detection** | **$983.6** | **$1,062.1** | **$918.3** | **$932.7** | **$989.9** | **$985.2** | **$989.4** | **$4,815.7** |
| **CPSS/CT/AT** | $91.5 | $241.7* | $123.8 | $129.0 | $160.2 | $163.3 | $165.9 | $742.1 |
| **AIT** | - | $30.5 | $29.1 | $28.8 | $30.1 | $29.2 | $30.1 | $147.3 |
| **ETD/Alarm Resolution Capability** | - | $23.8 | $26.8 | $26.5 | $37.9 | $28.9 | $24.8 | $144.9 |
| **PSP Legacy** | $185.2** | $16.0 | $10.3 | $12.4 | $12.3 | $12.3 | $12.7 | $6.0 |
| **EBSP** | $523.4 | $564.2 | $531.4 | $533.3 | $535.1 | $535.7 | $539.1 | $2,674.6 |
| **Canine** | $164.6 | $166.9 | $170.7 | $171.2 | $171.2 | $172.7 | $174.9 | $860.6 |
| **Counter-UAS (C-UAS)** | $0 | $0.0 | $3.0 | $8.2 | $19.7 | $19.8 | $18.5 | $69.2 |
| **Air Cargo** | $10.9 | $10.9 | $15.2 | $15.4 | $15.4 | $15.4 | $15.4 | $76.9 |
| **Surface** | $8.0 | $8.0 | $8.0 | $8.0 | $8.0 | $8.0 | $8.0 | $40.0 |
| **IT Systems Improvement** | **$375.0** | **$364.0** | **$369.3** | **$359.4** | **$358.2** | **$358.0** | **$358.2** | **$1,803.1** |
| **STIP** | $5.4 | $9.9 | $12.3 | $13.9 | $12.7 | $12.9 | $13.2 | $65.0 |
| **ITIP** | $369.6 | $354.1 | $357.0 | $345.5 | $345.5 | $345.0 | $345.0 | $1,738.0 |
| **Total** | **$1,491.0** | **$1,560.0** | **$1,428.1** | **$1,425.7** | **$1,465.0** | **$1,460.7** | **$1,467.0** | **$7,246.5** |

** The FY 2020 President's Budget for CT included $49.8 million from the Aviation Security Capital Fund.*
*** Passenger Screening Program (PSP) breakout into separate elements was initiated in the FY 2020 Resource Allocation Process; therefore, the FY 2019 Enacted only shows the total within PSP for CAT, AIT, AT, ETD, and PSP Legacy.*

[1] Because of rounding, numbers presented throughout this report may not add precisely to the totals indicated.

# Capital Investment Plan
# FY 2021–FY 2025

## Table of Contents

# I. Legislative Language

This report addresses reporting requirements in section 223 of the Fiscal Year (FY) 2020 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-93), as well as in the accompanying Joint Explanatory Statement and House Report 116-180, and the Transportation Security Acquisition Reform Act (P.L. 113-245).

P.L. 116-93 states the following:

> SEC. 223. 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 (CIP) 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 223 of the bill provides direction for capital investment plan requirements in lieu of language included in the House Report.

The Joint Explanatory Statement also states:

> Section 223. The agreement contains a new provision requiring TSA to provide a report that includes the Capital Improvement Plan, technology investment and Advanced Integrated Screening Technology. This includes the requirement in the House Report for a report on future year capital investment plan.

House Report 116-180 states:

> *Future-year Capital Investment Plan.*—TSA is directed to provide a report to the Committee, not later than 90 days after the date of enactment of this Act, on a future-year capital investment plan for procurement of new and replacement transportation security equipment.

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 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 Transportation Security Administration's (TSA) mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. To accomplish this, TSA has set ambitious goals for itself over the coming years as outlined in the FY 2018–2026 TSA Strategy. To ensure that TSA is well-equipped to implement this strategy and to sustain and modernize its operations, TSA considers the overall transportation environment, current and future risks and threats, and opportunities for collaboration with industry. TSA follows a structured and repeatable planning, programming, budgeting, execution, and strategy (PPBE-S) framework to identify the requirements necessary to address identified challenges such as an evolving threat landscape, increases in passenger volume, and budgetary constraints.

The CIP summarizes the output of TSA's efforts to plan strategically for and to enable continuous improvement in transportation security, specifically with transportation security equipment (TSE). The funding identified includes amounts for Procurement, Construction, and Improvement (PC&I); Operations and Sustainment (O&S); and Research and Development (R&D) as requested in the FY 2021 President's Budget and the outyear requirements in the Future Years Homeland Security Plan (FYHSP).

# III. Strategic Priorities

TSA has three mutually reinforcing guidance documents that drive TSA toward its strategic vision:

- The TSA Strategy,[2] which articulates the shared vision, goals, and priorities for TSA.
- Administrator's Intent,[3] which identifies near-term activities to advance the strategy.
- The FY 2022–FY 2026 Strategic Priorities and Planning Guidance, a key output of the Strategic Planning phase of the PPBE-S framework, which guides resource allocation decisions in subsequent outyear programming, budgeting, and execution phases.

As articulated in the TSA Strategy, TSA's strategic vision is driven by the following priorities:

- **Improve Security and Safeguard the Transportation System:** TSA will lead by example by strengthening operations through powerful and adaptable detection capabilities, intelligence-driven operations, and enhanced vetting. Strong partnerships across governments and industry will be integral to the success of this shared transportation security mission.

- **Accelerate Action:** TSA will build a culture of innovation that anticipates and rapidly counters the changing threats across the transportation system. TSA will mature its ability to make timely, data-driven decisions, and to field innovative solutions rapidly. TSA will simplify access for its partners and stakeholders to encourage robust collaboration.

- **Commit to Our People:** TSA's most important assets are the dedicated professionals securing our Nation's transportation system. TSA will foster a diverse, inclusive, and transparent work environment, establishing TSA as a federal employer of choice. TSA will transform its organizational culture to promote an entrepreneurial spirit and operational excellence.

Committed to an innovative vision that evolves to anticipate emerging threats, TSA is rethinking and transforming how it provides transportation security; is redesigning how TSA and its partners collect, protect, share, and use data; and is reevaluating how TSA engages with industry to develop and deploy innovative solutions. To accomplish this, TSA makes continuous and sustained capital investments in alignment with the following pillars:

- **Transportation Vetting and Identity Management:** Investment in TSA vetting of passengers and credential applicants and holders is essential to TSA's ability to identify and mitigate potential security risks in advance of travel or related to insider access.

[2] TSA Strategy, 2018–2026 <https://www.tsa.gov/sites/default/files/tsa_strategy.pdf>
[3] TSA Administrator's Intent, 2018 <https://www.tsa.gov/sites/default/files/tsaadminintent_2018.pdf>

- **Enhanced Threat Detection:** TSA must invest heavily in the primary and secondary screening of people and property across the transportation infrastructure. TSA can provide enhanced security by increasing its threat detection capabilities to screen more effectively in the checkpoint and checked baggage environments.

- **Information Technology (IT) Systems Improvement:** TSA is charged with securing the Nation's transportation systems from all threats, including cyber-attacks. TSA prioritizes identifying cybersecurity risks, reducing vulnerabilities to systems and critical infrastructure across the Transportation Systems Sector, mitigating consequences when incidents occur, ensuring the resiliency of the system, and creating greater flexibility.

To advance these pillars, TSA prioritizes continuous engagement with stakeholders and partners across governments, industry, and the traveling public.

# IV. System Context

Every checkpoint at every federalized airport serves as an entry point into the aviation system. Airports must function consistently to protect the entire system or there will be exploitable gaps in the security network. To combat this threat, TSA continues to operate year-round across more than 440 airports.

During FY 2019, TSA screened approximately 839 million aviation passengers, 1.9 billion carry-on items, and more than 510 million checked bags. This is a 4.3-percent increase in checkpoint volume and an average increase of 95,764 passengers per day over the prior fiscal year, with the increase in passenger growth expected to continue. The International Air Transport Association's 20-Year Air Passenger Forecast projects that the number of anticipated passengers screened in the United States will grow 2.4 percent annually over the next 20 years, reaching a total of 1.4 billion by 2037.[4] In the coming years, TSA will face the challenge of screening an increasing volume of passengers without compromising screening effectiveness within a physically constrained airport infrastructure.

The profile of the traveling public continues to evolve, requiring innovative and inclusive solutions from TSA. Globalization, an aging population, and a growing emphasis on passenger experience will continue to alter the transportation environment. Globalization contributes to an increase in overseas travel, with 81.3 million international travelers visiting the United States in 2018 alone, a 6-percent increase from the previous year.[5] This trend is projected to continue, providing the opportunity for new adversaries and threat areas to emerge across transportation modes. The percentage of the population ages 65 and older in the United States is expected to increase from 15 percent in 2018 to 22 percent in 2050; TSA will need more inclusive screening technology and procedures across transportation modes to respond.[6] TSA's security capabilities must scale to keep pace with these increased demands and to ensure that it continues to lead transportation security.

TSA also facilitates security across the Nation's other transportation modes, primarily focusing on oversight, cooperation, and regulation of the surface transportation environment. TSA must screen 100 percent of cargo transported on passenger aircraft at a level of security equal with the level of security for the screening of passengers' checked baggage. TSA regulates cargo screening technologies through the Air Cargo Screening Technology List. For the very high-risk mass transit and passenger rail, freight rail, pipeline, maritime terminals, transportation public areas, and infrastructure protection of all transportation modes, TSA stimulates the marketplace and evaluates and communicates technologies' effectiveness to streamline end-users' access to advanced and proven capabilities.

[4] International Air Transport Association report, "Passenger Forecast" (2017).
[5] U.S. Travel, "U.S. Travel's Research Trends." December 2018: Economic Overview (2018).
[6] Population Reference Bureau report, "2018 World Population Data Sheet" (2018).

"History has shown that terrorists will adapt their tactics and techniques in an attempt to bypass increased security procedures and are capable of developing increasingly sophisticated measures in an attempt to avoid detection."[7] This ever-changing threat necessitates continued investment into new technologies and the fielding of these technologies to strengthen transportation security. As terrorist tactics continue to evolve, there becomes a clear need for capital investment funding to mitigate risks present in TSA's domain.

## A. Identifying Threats

To meet evolving security threats and changes within the aviation industry, TSA continually adapts security screening capabilities as well as its inspections and compliance programs. Using intelligence reporting and analysis, modeling, and simulation capabilities, TSA calculates, ranks, and compares risks to the transportation sector, and provides leadership with a comprehensive understanding of the transportation sector's terrorism and other risk landscapes. Considered alongside other factors affecting TSA's system-level environment, these risk assessments help to identify and prioritize capability deficiencies, and help to make informed strategic and tactical investment decisions.

**Transportation Security Capability Analysis Process (TSCAP):** TSCAP is a structured, repeatable, and transparent process for evaluating the current security system, identifying a prioritized listing of capability gaps, and recommending courses of action to close these gaps. TSCAP continues to evolve to support TSA's mission and the DHS Joint Requirements Integration and Management System process. TSCAP helps senior leadership to identify optimal courses of action to close capability gaps, assists in TSA's PPBE-S process, and provides a key input to TSA's Technology Investment Framework (see Appendix, Section IV).

**Risk and Trade Space Portfolio Analysis (RTSPA):** RTSPA provides TSA with an annual assessment of security effectiveness of checkpoint and checked baggage capabilities against a known threat spectrum, and identifies areas for system enhancement. TSA leadership leverages RTSPA results to make decisions regarding potential changes in procedures and security technology, to evaluate the effectiveness of the overall security system against emerging threats, and to determine the potential impacts of future changes.

## B. Transportation Security Equipment Acquisition Update

This section compares security-related technology (SRT)[8] acquired since 2017 against the planned technology programs and projects in the 2017 Refresh per requirement (g2) of the Transportation Security Acquisition Reform Act (P.L. 113-245).

---

[7] U.S. Government Accountability Office (GAO) report, "Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain," (GAO-06-371T) (2006).

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

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 the development and deployment of enhanced threat detection performance and alarm-resolution capabilities. When upgrades are not achievable to mitigate obsolescence, recapitalization remains the sole solution.

The following acquisitions deviated from the 2017 Refresh and other TSA projections:

- **Credential Authentication Technology (CAT) Units in FY 2019:** In September 2018, TSA completed initial operational test and evaluation (T&E) to support an acquisition review board decision in February 2019 to declare initial operating capability on the original 47 low-rate initial production units. TSA completed follow-on operational testing and evaluation in early August 2019 on the Windows 10 operating system version of the CAT unit and achieved acquisition decision event (ADE) approval in late August 2019 to produce and deploy the first 505 CAT units. TSA procured 505 units instead of 294 units in FY 2019 to accelerate CAT deployments to reach full operational capability prior to FY 2022.

- **Computed Tomography (CT) Units in FY 2019:** TSA procured 300 advanced technology X-ray (AT)/CT units as a project under the AT program. These AT/CT units are an initial increment to get CT capabilities into the field at high-priority airports quickly, while TSA stands up the Checkpoint Property Screening System (CPPS) Program as the long-term solution. CPSS achieved ADE 2A approval in August 2019, and AT/CT units will be moved under CPSS for management and sustainment.

- **AT Units in FY 2017:** Equipment requirements changed, and the funding allotted for ATs in FY 2017 was reallocated to other priority initiatives. TSA does not plan to procure additional AT units, except "as needed" to address airport passenger growth and urgent screening equipment needs.

- **Explosives Detection Systems (EDS) Units in FY 2019:** TSA procured 65 EDS units in FY 2019 to support recapitalization efforts and deployment of new inline screening systems. Procurement quantities are based on airport equipment requirements and are dependent on the timelines for project execution at each specific airport site.

- **Advanced Imaging Technology (AIT) Units in FY 2017**: TSA procured 15 AIT units in FY 2017 for safety stock. In late FY 2019, TSA procured 100 AIT units for airport expansion and to fulfill many small airport needs.

Additionally, TSA awarded contracts for the technologies outlined in Figure 6 during FY 2019.

***Figure A1: TSA Transportation Security Equipment (TSE) Awards, October 2018–September 2019***

| TSE | Number Awarded | Timeframe |
|---|---|---|
| **AIT** | 100 | September 2019 |
| **AT/CT** | 300 | March 2019 |
| **Boarding Pass Scanner (BPS)** | 100 | March 2019 |
| **CAT** | 505 | February 2019, July 2019 |
| **EDS** | 65 | September 2019 |

## C. Mitigating Threats

### Transportation Vetting and Identity Management

Vetting is the initial point of contact to identify potential threats from individuals seeking access to our transportation environment as passengers or as credential holders with insider access. TSA conducts 24/7 recurrent vetting for more than 2.2 million daily passengers flying into, out of, or over the United States, as well as recurrent vetting for more than 20 million credential holders including TSA Pre✓®, airport, airline, flight crew, air cargo, maritime, and certain surface transportation populations. TSA's vetting approach is to focus on identifying individuals of greater risk so that they can receive enhanced physical screening. TSA's vetting approach also focuses on identifying credential applicants and holders who have insider access and who may pose a risk so that appropriate action can be taken. This approach enables TSA to apply appropriate levels of physical screening or other actions based on the individual's assessed level of risk.

For the airport checkpoint, deploying CAT allows TSA to authenticate the security features present on passenger identification documents (ID). It also allows TSA to verify a passenger's vetting status against the TSA Secure Flight system in near real-time so that the passenger receives the appropriate screening based on TSA's assessed risk.

TSA seeks to mature its risk-based approach to increase the use of biometrics screening, improving confidence in security verification and minimizing the risk of adversary manipulation. In 2018, TSA published the "Biometrics Roadmap for Aviation Security and the Passenger Experience", establishing its plans for the use of biometrics to improve both security and the travel experience, while safeguarding the Nation's transportation system and accelerating the speed of action through smart investments and collaborative partnerships.[9] Implementing biometrics technology at the checkpoint could expand the ability to detect adversaries from seeking, and to deter adversaries from attempting, to obtain less-rigorous screening, as well as to decrease checkpoint cycle time.

Figure 7 shows the funding aligned to transportation vetting and identity management projects and programs from the FY 2021 congressional justification and TSA's FY 2021–FY 2025

[9] TSA Biometrics Roadmap for Aviation Security and the Passenger Experience, September 2018 <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf>.

FYHSP. SRT[10] programs are noted for the 5-year technology investment plan requirements traceability.

***Figure 7: Transportation Vetting and Identity Management FY 2021–FY 2025***

| Transportation Vetting and Identity Management – Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$140.5** | **$133.6** | **$116.9** | **$117.4** | **$119.4** |
| Secure Flight | $117.9 | $121.6 | $106.5 | $107.6 | $109.3 |
| CAT[11] | $20.6 | $10.0 | $5.4 | $4.7 | $5.1 |
| Biometrics Technology | $2.0 | $2.0 | $5.0 | $5.0 | $5.0 |
| **Total** | **$140.5** | **$133.6** | **$116.9** | **$117.4** | **$119.4** |

## Enhanced Threat Detection

The checkpoint system addresses emerging and evolving terrorist threats to commercial aviation security. To address the continued spread of improvised explosive threats, greater numbers of weapons found at checkpoints, and expanding passenger throughput, TSA continues to improve automated threat detection and alarm resolution capabilities while streamlining security operations for increased throughput.

To outmatch the expanding threat, TSA invests in enhanced technologies and processes to strengthen operational effectiveness. One such example is the recent deployment of CT systems, which offer an enhanced imaging platform compared to legacy AT and can detect a broader range of threats.

The threat environment for checked baggage includes military, commercial, and homemade explosives. TSA continues to screen 100 percent of checked baggage for explosive threats, as required by the Aviation and Transportation Security Act (ATSA). TSA mitigates vulnerabilities in the checked baggage environment with EDS, which use CT technology to screen checked baggage, and Explosive Trace Detection (ETD) units, which detect a wide range of explosives threats.

Figure 8 shows the funding aligned to enhanced threat detection projects and programs from the FY 2021 congressional justification and TSA's FY 2021–FY 2025 FYHSP.

***Figure 8: Enhanced Threat Detection FY 202 –FY 2025***

| Enhanced Threat Detection – Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total PC&I** | **$283.4** | **$282.1** | **$283.2** | **$285.2** | **$281.2** |

[10] SRT is defined as any technology or related engineering services to deployed technology that assists the Administration 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.

[11] These programs are SRT programs.

| Enhanced Threat Detection – Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| Checkpoint Property Screening System (CPSS)/CT[12] | $28.9 | $29.0 | $29.0 | $29.0 | $29.0 |
| Electronic Baggage Screening Program (EBSP)[12] | $254.5 | $253.1 | $254.2 | $256.2 | $252.2 |
| **Total O&S** | **$626.9** | **$642.6** | **$680.2** | **$685.3** | **$700.7** |
| AT and CPSS/CT[12] [13] | $94.9 | $100.0 | $131.2 | $134.3 | $136.9 |
| EBSP[12] | $276.9 | $280.2 | $280.9 | $279.5 | $286.9 |
| AIT[12] | $24.1 | $23.8 | $17.4 | $19.4 | $22.6 |
| ETD[12] | $23.8 | $23.5 | $24.1 | $24.0 | $24.8 |
| Passenger Screening Program (PSP) Legacy[12] | $10.3 | $12.4 | $12.3 | $12.3 | $12.7 |
| TSA-Led National Explosives Detection Canine Teams | $135.9 | $136.3 | $136.4 | $137.8 | $140.1 |
| State and Local Law Enforcement Explosives Detection Canine Teams | $34.8 | $34.8 | $34.8 | $34.8 | $34.8 |
| Counter-Unmanned Aircraft System (C-UAS) | $3.0 | $8.2 | $19.7 | $19.8 | $18.5 |
| Air Cargo | $15.2 | $15.4 | $15.4 | $15.4 | $15.4 |
| Surface | $8.0 | $8.0 | $8.0 | $8.0 | $8.0 |
| **Total R&D** | **$8.0** | **$8.0** | **$26.5** | **$14.7** | **$7.5** |
| On-Person Screening Capability[12] | $5.0 | $5.0 | $12.7 | $9.8 | $7.5 |
| Alarm Resolution Capability[12] | $3.0 | $3.0 | $13.8 | $4.9 | - |
| **Total** | **$918.3** | **$932.7** | **$989.9** | **$985.3** | **$989.4** |

**IT Systems Improvement**

TSA continues to protect the confidentiality, integrity, and availability of its systems, data, and information by staying ahead of cyber threats and by modernizing its IT systems. TSA also needs to respond rapidly to the threat environment and to engage with its sector stakeholders to ensure that it understands the vulnerabilities in the transportation system. To be proactive in these efforts, TSA developed a Cybersecurity Roadmap, which aligns with the National Cyber Strategy and the DHS Cybersecurity Strategy. It provides the framework for TSA to secure its internal systems and to ensure the resiliency of the transportation system to cyberattacks.[14]

IT systems improvement investments are interdependent with other technology investments to improve TSA's effectiveness and efficiency. For example, machine-learning algorithms could automate and increase performance in many repetitive, labor-intensive tasks, but collecting data to support the development of machine-learning algorithms is impractical without networked TSE. The Security Technology Integrated Program (STIP) will provide this connectivity, enabling the automated exchange of information between TSE across the TSA network and the

[12] These programs are SRT programs.
[13] AT and CPSS/CT are currently listed under one investment. This will change in the new reporting cycle when the CPSS/CT and AT programs become separate investments.
[14] The TSA Cybersecurity Roadmap can be found at https://www.tsa.gov/about/strategy under "Key Documents."

sharing of real-time performance data across environments. Cybersecurity is foundational to networking TSE, so under-investment in either cybersecurity or its interdependent technologies limits the ability to develop and deploy more advanced capabilities and screening enhancements.

Figure 9 shows the funding aligned to IT Systems Improvement projects and programs from the FY 2021 congressional justification and TSA's FY 2021–FY 2025 FYHSP.

***Figure 9: IT Systems Improvement FY 2021–FY 2025***

| IT Systems Improvement – Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$369.3** | **$359.4** | **$358.2** | **$358.0** | **$358.2** |
| STIP | $12.3 | $13.9 | $12.7 | $12.9 | $13.2 |
| IT Infrastructure Program | $357.0 | $345.5 | $345.5 | $345.0 | $345.0 |
| **Total** | **$369.2** | **$359.4** | **$358.2** | **$358.0** | **$358.2** |

## D. TSA's Future State

The U.S. transportation system always will be a target, and consequently always will need protection. A primary attraction for adversaries is its vast size and openness, as well as the consequence of an attack to our national psyche. This means a small adversary investment in an attack can result in a disproportionate economic and emotional impact. In TSA's future state, advances in defensive technology will overcome these inherent disadvantages and will deter or defeat attacks against the transportation system.

Reaching this future state requires better analytics and differentiation between Trusted Travelers and those who present higher risk. It also requires more connected and agile security equipment that can adapt to new threats rapidly. 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, are needed for long-term improvements in TSA's overall performance.

TSA already has made steps toward its future state and will continue progress by introducing Open System Architecture Elements to increase efficiency and interoperability across TSE and screening systems. The Checkpoint Automation project (formerly known as Open Threat Assessment Platform) is exploring proofs-of-concept to decouple the hardware and software development lifecycles, which promotes increased competition and innovation of threat detection capabilities.

### Capability Management

To meet the increasing security demands of transportation systems better, TSA is transitioning to a capability management operating model to improve integration and to take a more comprehensive approach to security solutions. TSA aligns capability managers by function/capability, not by acquisition program. They are responsible for leading doctrine,

organization, training, matériel, leadership, personnel, and facilities plus requirements, grants, and standards analysis at the early stages of a capability's development. This allows them to direct early-stage capability development, to inform resource allocation decisions better, to maintain oversight across the TSA Acquisition Lifecycle Framework, and to continue support into sustainment.

TSA capability managers are aligned to the following portfolios:

- **Accessible Property:** Enhancing the security effectiveness and operational efficiency of TSA's accessible property screening through automation, integration, and connection.

- **Identity Management 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.

- **Alarm Resolution:** Advancing matériel and nonmatériel capabilities to identify, analyze, and resolve alarms accurately within the TSA security ecosystem.

- **On-Person Screening:** Improving TSA's on-person screening capabilities, including AIT, walk-through metal detectors, pat-down procedures, and other emerging capabilities.

- **Checked Baggage:** Advancing effective and efficient matériel and nonmatériel solutions in the checked baggage space.

- **Multimodal:** Providing security technology recommendations and solutions for air cargo, public transportation areas, and critical infrastructure (e.g., pipelines) by evaluating existing security technologies, by developing requirements for new technologies, and by stimulating the technology marketplace.

- **Counter Unmanned Aerial Systems:** 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.

- **Field Information Systems:** Collaborating with field security operations stakeholders to innovate and advance field information systems that support security information gathering and information sharing among DHS, TSA, law enforcement, and intelligence community stakeholders.

## E. Research and Development

The U.S. transportation system operates in a dynamic risk environment characterized by sudden change and terrorist adaptation. TSA's ability to respond to known or emerging threats with timely solutions depends on sustained and coordinated investment in research, development, test, and evaluation.

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

TSA works with DHS S&T to inform and shape capability development throughout the acquisition process by supporting capability gap identification, requirements definition, test and evaluation (T&E) execution, 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 across the Nation's other transportation modes (mass transit and passenger rail, freight rail, pipeline, maritime terminals, transportation public areas, and infrastructure protection of all transportation modes) by evaluating and communicating a technology's effectiveness, thereby stimulating the marketplace and streamlining end-user access to advanced and proven capabilities. In collaboration with the Johns Hopkins University Applied Physics Laboratory and other Federal Government and nongovernment entities (such as laboratories, technical centers, and industry partners), TSA assesses leading security capabilities and communicates results to key stakeholders to spark innovation within the surface transportation marketplace.

## F. Priority Areas for Investment

TSA applies systems and risk analyses to identify critical systems or functional areas for prioritized investment based on the greatest risk and opportunity for improvement. Investing only in these areas, however, leaves many other opportunities for improvement unfulfilled. Individual capabilities may be less effective if partially funded as a piecemeal solution, rather than ones deliberately developed in partnership with other related capabilities. Under present funding constraints, TSA has prioritized investments in property screening, property threat resolution, and on-person screening capabilities because they present the largest risk-based opportunities for security improvement.

**Property Screening Capabilities:** The security effectiveness and operational efficiency of TSA's current property screening technologies could be improved by investments in the following areas:

- Acquisition of improved versions of existing technologies,
- Development of enhanced/extended versions of existing technologies, including making data from sensors available for algorithm development,
- R&D to detect a wider range of improvised threats, and
- R&D to improve discrimination of threats and benign objects.

**Property Threat Resolution Capabilities:** TSA's current property threat-resolution technologies are relatively old and limited in their capabilities. Even with current efforts to improve primary property screening capabilities (for example, CT systems for carry-on baggage and EDS for checked baggage), improvements to security effectiveness will remain limited unless threat-resolution capabilities are improved as well. Opportunities include investments in:

- Acquisition of improved versions of existing technologies,
- R&D for new sensors to resolve a wider range of threats at trace levels, and
- R&D to enable detection/discrimination of bulk materials (without requiring access to or samples of the material in question).

**On-Person Primary Screening Capability:** AIT systems are currently TSA's best on-person screening detection technology; however, many have been deployed for almost a decade and they take up significant space in the checkpoint. Their limited throughput represents a significant bottleneck, failing to keep up with increasing passenger volume. To enable AIT screening of a larger share of passengers, TSA will conduct R&D and work with vendors to develop and acquire faster and smaller next-generation AITs. In the meantime, opportunities to improve security effectiveness through enhanced capability include the following:

- Retrofit AIT units to enhance detection performance, to reduce false alarms, and to extend useful life; and
- Continue to purchase additional current AIT units as TSA adds new checkpoint lanes.

In addition, TSA will invest in new technology that can detect threats concealed within a passenger's body and can discriminate between those threats and medical implants. TSA also will invest in R&D for beyond "next generation" on-person screening technologies that can screen passengers automatically at speed, can detect reduced threat masses, and can discriminate between different materials.

**Security System Integration and Information Sharing Capabilities:** Improvements to security effectiveness and operational efficiency will remain limited unless enhancements to support integration and networking of technologies are improved as well. Opportunities include investing in the following:

- Development of common, accessible sensor, operator, and network interfaces for existing technologies;
- Checkpoint information management, including incident reporting; and
- R&D to develop hardware and software for integrating data from multiple sensors and other data sources to improve security system performance and efficiency at local, regional, and national levels.

As aviation security screening demands increase with growing passenger volume, there is a need to implement a risk-based aviation security approach that verifies the identity and obtains the risk level of 100 percent of travelers. Opportunities include investing in biometrics technology through enhancements to CAT and other systems, and collection of biometrics to verify identity at the checkpoint.

## G. Partnerships and Collaboration

TSA constantly seeks ways to collaborate better with partners from industry, government, and academia to improve security effectiveness, operational efficiency, passenger experience, and workforce capabilities. These initiatives include the following:

**International Collaboration:** TSA works to establish 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. Maintaining open dialogue helps TSA and its partners to build and enforce joint standards, to align R&D efforts, and to test emerging capabilities, ultimately improving the overall global security landscape.

**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. With more information about the traveling public, via expanded TSA Pre✓® enrollment, security measures can be more tailored to the specific individual. TSA can screen travelers through TSA Pre✓® lanes at a rate of about 240 per hour, compared to 140 to 150 travelers per hour at standard screening lanes.

**Developing New and Improve Current Capabilities:** TSA works 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 to identify emerging technologies that can improve security, the passenger experience, and efficiency, and then to pilot these new technologies and capabilities in live field environments.

**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 can enhance performance for AT, CT, EDS, and AIT. These new algorithms use machine-learning approaches to discriminate between threats and benign objects, making the screening process more effective and efficient. TSA anticipates that machine-learning algorithms not only will improve security effectiveness, but also will support automation in future security systems and will reduce false alarm rates. This will enhance operational efficiency further and improve the passenger experience.

**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. It provides TSA with an avenue to work with industry to demonstrate flexible, mature, and standardized "curb-to-gate" security solutions and techniques for transportation infrastructure, demonstrating these solutions and techniques in an operational environment to ensure that they are viable in the intended environment. 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 can be procured through grants programs or can be purchased with confidence by users nationwide.

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

**Capability Acceptance Process:** TSA developed the capability acceptance process to facilitate receiving capabilities such as TSE and other technologies from industry stakeholders and partners. It provides an objective and repeatable process to evaluate, accept, and implement requests to offer capabilities outlining 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 who may benefit from accelerating procurement and deployment timelines, recapitalizing TSE, and/or enhancing security and the passenger experience.

# V. Conclusion

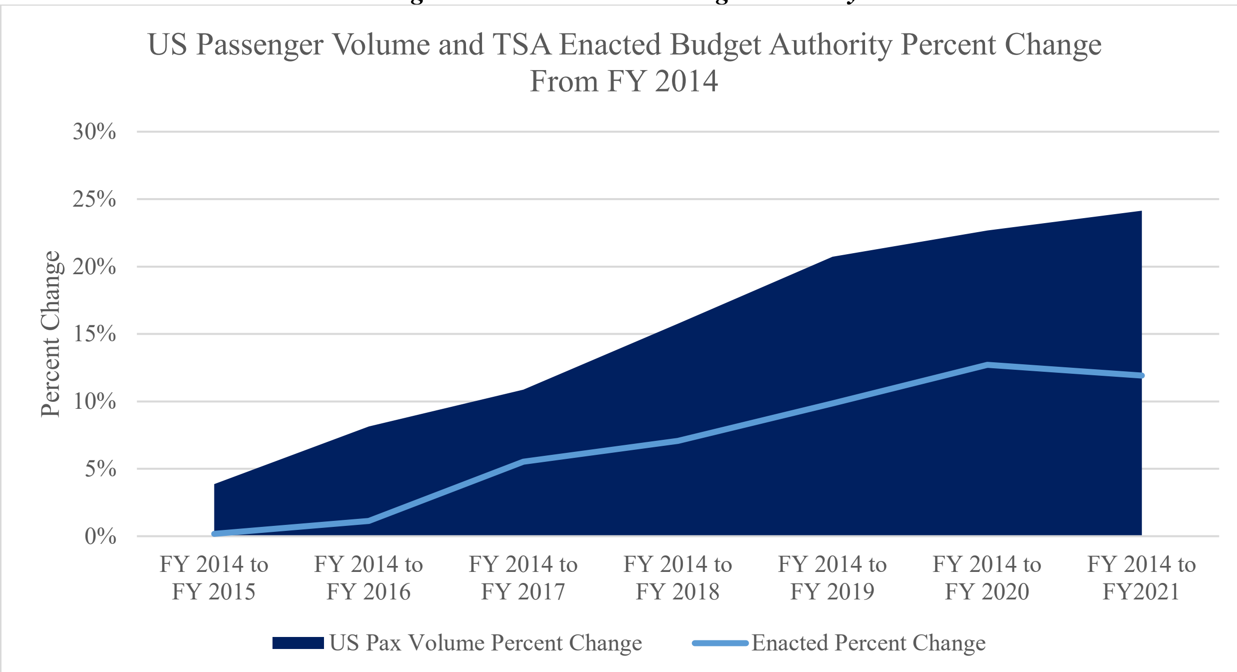
TSA relies on federal funding through appropriated dollars and passenger fees. During TSA's early years, capital investment funding was a significant proportion of the TSA portfolio to build out its infrastructure. Resource flexibility, specifically TSA's 2-year appropriation, provided to TSA the ability to manage multiyear investments using carryover funds and to reprogram between different budget accounts to cover capital expenditures where needed.

To make full use of its resource flexibility and to maintain security for a growing traveling population, TSA must continue to identify and align resources to its priority mission needs. An increase in passenger volume and the changing demographic of travelers across all modes of transportation affect the way that TSA and our adversaries operate. TSA must invest in new technologies, techniques, and procedures to stay ahead of these adversaries and to prepare for shifting traveler demographics.

Although TSA continues to achieve its national security mission within the limits of its current financial model, an inverse relationship is growing between funding aligned to the security mission and the increase in volume of passengers that require security screening. As noted in Figure 10: TSA Enacted Budget Authority, although the number of travelers continues to grow, TSA's funding has not increased by the same percentage growth as passenger volume. Given this budget reality, TSA has prioritized funding toward maintaining required operational levels, as well as funding additional manpower to ensure that wait times are maintained at appropriate levels.

Much of the TSE forming TSA's physical security infrastructure is almost a decade old and is approaching obsolescence. The infusion of capital investment outlined in this capital investment plan will help TSA to update and upgrade aging equipment and to incorporate capabilities that can defeat and deter emerging threats at the checkpoint and across the aviation sector.

***Figure 10:  TSA Enacted Budget Authority***




Despite a relatively flat topline, the FY 2021 TSA Budget includes funds for investment programs to maintain, purchase, and deploy CT and CAT units, to address retention for transportation security personnel, to continue building a cybersecurity workforce, and to support the increasing maintenance costs of TSE.  TSA also is funding the development of next-generation AIT units, emerging alarm-resolution technologies, and biometrics.

As TSA's risk landscape evolves, it must continue to invest in acquiring and fielding new technologies to strengthen transportation security.  The capital investments identified in the CIP are designed to position TSA to meet the challenges of an evolving threat landscape and shifts in passenger volume and traveler demographics while operating in a fiscally constrained environment.  The CIP provides a guide to TSA's investment approach and informs future trade-offs between maintaining current operations and investing in acquiring and fielding new technologies to strengthen transportation security.  By considering the overall transportation environment, the current and future risks and threats it faces, and opportunities for collaboration with industry, the CIP helps ensure that TSA is better equipped to identify the capital requirements necessary to address identified challenges and risks.

[THIS PAGE INTENTIONALLY LEFT BLANK]

# Appendix

# I. Transportation Security Equipment Programs

This section covers only security-related technology (SRT) programs to consolidate information pertaining to the requirements of the 5-year Technology Investment Plan and the Advanced Integrated Passenger Screening Technologies report. Additional projects and programs discussed in the Capital Investment Plan (CIP) are included in a later section.

## A. Credential Authentication Technology

**Overview**

***Illustration of CAT Machine***

Credential Authentication Technology (CAT) provides a primary means for authenticating identification document (ID) security features that passengers present to transportation security officers (TSO) before the passengers enter the passenger screening checkpoint, and for determining the Secure Flight vetting status for the passenger.

The Transportation Security Administration (TSA) currently relies on a manual process to authenticate various forms of identification presented by passengers, airport/airline personnel, and law enforcement officers. With new features that require use of magnification, however, travel document checkers (TDC) have a greater need for enhanced tools to help them validate security features. Although REAL ID will help to standardize and elevate the security features of IDs to make counterfeiting more difficult, the TDCs will need an enhanced tool to allow them to verify those security features.

**Objectives and Goals**

CAT closes current security gaps and enhances the passenger screening process at the checkpoint by improving the inspection of IDs and confirming passengers' vetting status. The CAT Program has three primary objectives:

- Enhance the ability to verify a passenger's ID accurately,
- Enhance the ability to validate a passenger's flight reservation status accurately, and
- Enhance the ability to verify a passenger's Secure Flight vetting status accurately.

CAT has two major milestones expected between Fiscal Year (FY) 2020–FY 2025, dependent on availability of funds:

- Deploy REAL ID enhancements capability by early Q4 FY 2020, and
- Achieve full operational capability (FOC) by FY 2022.

### Security Capability

Identity verification is important to sterile area security to ensure that passengers traveling into and within the United States are not attempting to avoid identification for malicious or other reasons. TSA established CAT to scan and validate consistently and efficiently the authenticity of passenger-provided ID credentials, such as driver’s licenses and passports. CAT is also able to verify the biographic information on a passenger’s ID with their associated Secure Flight prescreening status (Pre✓®, Standard, or selectee).

CAT will play a critical role in ensuring that passengers receive the screening procedures appropriate to their risk level, supporting the congressional mandate that requires TSA to segment passengers by March 2020. To ensure that only identified low-risk passengers receive the new modified screening procedures, the modified lane will leverage CAT units to validate travelers’ identities.

The CAT document library now can authenticate newly designed and issued REAL ID-compliant identifications. TSA will implement software enhancements to alert the TDC when a traveler presents a noncompliant driver’s license. In addition, as states look to advance the national standard and issue mobile drivers’ licenses (a digital version of an individual’s driver’s license stored on a smart phone), hardware and software enhancements to CAT will be developed to enable the system to authenticate mobile driver’s licenses.

### Interdependencies/Related Investment

Identity verification is the foundation of all Trusted Traveler initiatives. Until biometric identity verification is in place, CAT will provide the core identity verification capability for checkpoints. CAT also will be a prerequisite to enable some of the more efficient screening processes that TSA is considering, such as Future Lane Experience Screening (FLEx).

CAT is interdependent with the Security Technology Integrated Program (STIP), which focuses on the automated exchange of information between TSE across the TSA network, to draw passenger vetting statuses from Secure Flight. These vetting statuses allow the checkpoint to receive and act on additional passenger risk segmentation. Without STIP, CAT is only able to validate a passenger’s ID, not to verify their vetting status. CAT is the first technology built to use network connectivity for necessary functionality.

### Desired Future Capabilities

CAT is an improvement to current processes because it provides a clear alert when a passenger’s credential is potentially invalid, or when the identity information does not match the identity prescreened by Secure Flight. Developing a feedback mechanism for CAT to identify the normal versus abnormal variations in different state licenses and other credentials could increase the efficiency of the TDC station and improve detection of actual impostors.

## Funding Profile

Figure A1 contains funding to plan, procure, deploy, and maintain CAT equipment. Other operational needs may require increasing CAT units above the existing FOC.

***Figure A1: Credential Authentication Technology, FY 2021–FY 2025***

| CAT – Future Year Homeland Security Plan (FYHSP) Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total Operations and Sustainment (O&S)**[15] | $20.6 | $10.0 | $5.4 | $4.7 | $5.1 |
| **Total** | **$20.6** | **$10.0** | **$5.4** | **$4.7** | **$5.1** |

# B. Checkpoint Property Screening System/Computed Tomography

## Overview

Currently, the most capable carry-on baggage screening technology is the computed tomography (CT) system, which will provide security enhancements by finding a broad range of threats. CT systems offer an enhanced imaging platform compared to legacy advanced technology X-Ray (AT) and can be upgraded over time to detect an expanded library of emerging threats. TSA also plans to use CT units as prototypes for data collection, which will help to inform the CPSS requirements and to support algorithm development.

***Illustration of CT Machine***

TSA is pursing and sustaining four CPSS system configurations: AT/CT, CPSS Base, CPSS Mid-size, and CPSS Full-size. AT/CT systems are CT scanner-equipped with gravity rollers, ingress/egress conveyors, Primary Viewing Station (PVS), Alternative Viewing System (AVS), and a threat detection algorithm. AT/CT systems purchased under the AT Program have been transferred to the CPSS Program for management and sustainment. CPSS Base systems are CT scanner-equipped with gravity rollers, ingress/egress conveyors, PVS, AVS, a threat detection algorithm, and STIP Client Compatibility. CPSS Mid-size systems are CT scanners equipped with gravity rollers, ingress/egress conveyors, operator initiated auto divert capabilities, PVS, AVS, a threat detection algorithm, and STIP Client Compatibility. CPSS Full-size systems are CT scanners equipped with operator-initiated auto divert capabilities, automated bin conveyance system with parallel divestiture and recomposure, automated bin return, high-threat containment box, PVS, AVS, a threat detection algorithm, and STIP compatibility.

## Objectives and Goals

TSA stood up the TSA Checkpoint Property Screening System (CPSS) Acquisition Program in 2019 to deploy a long-term CT solution incrementally with enhanced threat detection algorithms, ingress/egress, and networking capabilities. This approach allows TSA to deploy an initial

[15] O&S funding includes maintenance and federal payroll costs. Maintenance accounts for 66 percent of total O&S.

capability and to expand functionality progressively until full capabilities are realized. The primary objective of CPSS is to deploy successful CPSS capabilities and to integrate them with existing security screening processes and technologies to outpace emerging threats, to improve security efficiency, and to improve the passenger experience. TSA's long-term goal is to employ checkpoint CPSSs with "auto-detect" capability for explosive threats and other prohibited items, such as firearms, firearm components, and knives. CPSS then would operate like EDSs for checked baggage, which only present an image for screeners when an alarm occurs. This capability could reduce staffing requirements and could improve checkpoint efficiency.

TSA will use an incremental acquisition strategy to deploy capability enhancements in block upgrades that support rapid acquisitions and increase operational efficiency. CPSS has three primary milestones between FY 2020–FY 2025, dependent on availability of funds:

- Deploy AT/CT systems to high-risk airports in FY 2020, and upgrade system algorithm to an advanced threat detection standard.

- CPSS Increment 1 (FY 2020-FY 2022): Procure and deploy CPSS configurations (base, mid- and full-size) with an advanced threat detection standard, and STIP compatibility. Mid-size configurations will have ingress/egress with automated diverter, and full-size configurations will have parallel divestiture, recomposure (with Auto Bin Return).

- CPSS Increment 2 (FY 2023-FY 2025): Procure and deploy CPSS configurations with an advanced threat detection standard and STIP connection (networked).

**Security Capability**

TSA is using an agile, innovative approach to procure and deploy CT at the checkpoint to address system integration and operational readiness rapidly, and to improve system performance. This approach allows TSA to deploy specific capabilities as part of a larger solution—progressively expanding functionality in the operational environment until CPSS reaches full capability.

**Interdependencies/Related Investments**

Initial CT deployments will require additional TSOs, but that requirement gradually will decrease over time. Because of interdependencies with automated screening lanes (ASL) to control the flow of articles into and out of the system, TSA will place both CT and ASL programs under the CPSS program in the future. CT systems also rely on STIP to push out algorithms and to conduct potential remote screening and review of images. Future investments also will leverage CT systems in the field for data collection and rapid development and deployment of advanced detection algorithms.

**Desired Future Capabilities**

CT checkpoint X-ray systems would benefit from modifications that substantially reduce false-alarm rates and enhance security capabilities, such as X-ray imaging system enhancement,

advanced algorithm development, system modeling and simulation, system standardization, threat characterization, and stream of commerce false-alarm reduction.

### Funding Profile

Figure A2 contains funding to plan, procure, deploy, and maintain CT systems.

***Figure A2: CPSS, FY 2021–FY 2025***

| CPSS – FYHSP Constrained, FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total PC&I** | **$28.9** | **$29.0** | **$29.0** | **$29.0** | **$29.0** |
| **Total O&S**[16][17] | **$94.9** | **$100.0** | **$131.2** | **$134.3** | **$136.9** |
| **Total** | **$123.8** | **$129.0** | **$160.2** | **$163.3** | **$165.9** |

## C. Electronic Baggage Screening Program

### Overview

The Aviation and Transportation Security Act (ATSA) of 2001 mandates that 100 percent of aviation checked baggage be screened by electronic or other approved means. TSA accomplishes this mission by testing, acquiring, deploying, integrating, upgrading, and maintaining technology that screens checked baggage. The fleet consists of approximately 2,638 Explosive Trace Detection (ETD) devices and 1,689 EDSs.

***Illustration of EDS***

Since the passage of ATSA in 2003, TSA's checked baggage focus has expanded to ensure that airports' screening zones for checked baggage use the most effective technologies. This effort requires the development and deployment of technology with improved performance. It also requires the integration of EDS equipment with airport baggage-handling systems to improve the efficiency of screening operations for checked baggage at many larger airports.

### Objectives and Goals

To meet the mandate continually, the Checked Baggage Technology Division manages one acquisition program, the Electronic Baggage Screening Program (EBSP), 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 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

[16] O&S funding includes maintenance and federal payroll costs. Maintenance accounts for 71 percent of total O&S.
[17] AT and CPSS/CT are listed under one investment. This will change in the new reporting cycle when the CPSS/CT and AT programs become separate investments.

effectiveness and to support operational need. EBSP has several key milestones planned for FY 2020–FY 2025, dependent on availability of funds:

- Recapitalize technically obsolete EDSs (FY 2020–FY 2024),
- Develop and deploy enhanced screening (FY 2020–FY 2024), and
- Define and map Federal Information Security Management Act (FISMA) boundaries and applicable cyber controls, and obtain authority to operate for legacy equipment (FY 2020–FY 2021).

**Security Capability**

TSA uses EDSs as the primary screening method for checked baggage. At airports that do not meet TSA's minimum requirement for EDS cost-effectiveness, TSA employs ETD for primary checked-baggage screening. TSA continues to work with industry to apply incremental approaches to technology development. This approach allows TSA to procure technologies and to upgrade existing machines as enhanced capabilities are available, 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 that improve security effectiveness by detecting additional threat materials and reduced threat mass, and by reducing the false-alarm rate,
- Define and manage cybersecurity compliance,
- Image format standardization and the use of machine-learning technology,
- On-screen alarm resolution in the checked-baggage resolution area,
- Common graphical user interface on EDS, which improves the performance of operators, and
- Recapitalization of technically obsolete EDS machines.

**Interdependencies/Related Investment**

TSA uses STIP to communicate with airport checked-baggage inspection systems. STIP imposes cybersecurity requirements for connectivity of checked-baggage TSE.

**Desired Future Capabilities**

To improve the performance and capability of existing checked-baggage screening systems, TSA continues to seek CT technology system enhancements. Further, as TSA continues to deploy CT systems for checkpoint operations, checked-baggage and checkpoint CT systems will be able to leverage investments in capability developments because they share a similar technology base. Future efforts in research and development (R&D) are focused on the following:

- EDS enhancement,
- Stream of commerce false-alarm reduction,
- Advanced algorithm development,
- Threat characterization, and
- System analysis and modeling.

**Funding Profile**

The costs identified in Figure A3 will allow TSA to test, procure, deploy, and maintain checked-baggage screening technologies and equipment with the latest threat detection capabilities.

***Figure A3: EBSP, FY 2021–FY 2025***

| **EBSP – Explosives Detection Systems – FYHSP Constrained FY 2021–FY 2025 ($M)** | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total PC&I** | **$254.5** | **$253.1** | **$254.2** | **$256.2** | **$252.2** |
| EBSP | $4.5 | $3.1 | $4.2 | $6.2 | $2.2 |
| Aviation Security Capital Fund | $250.0 | $250.0 | $250.0 | $250.0 | $250.0 |
| **Total O&S[18]** | **$276.9** | **$280.2** | **$280.9** | **$279.5** | **$286.9** |
| **Total** | **$531.4** | **$533.3** | **$535.1** | **$535.7** | **$539.1** |

## D. Advanced Imaging Technology

***Illustration of AIT***

**Overview**

TSA identifies, tests, procures, deploys, and sustains equipment that detects threats concealed on passengers as they enter the screening checkpoint. Advanced Imaging Technology (AIT) systems use millimeter wave technology to identify undivested items on persons in seconds. This technology serves as an increased detection capability that identifies metallic and nonmetallic threats and reduces physical patdowns at security checkpoints.

**Objectives and Goals**

The AIT program goal is to enhance the travelers' experience while improving security, by achieving a higher detection and lower false-alarm system that uses a gender-neutral algorithm. AIT has three primary planned milestones between FY 2020–FY 2025, dependent on availability of funds:

- Next-generation on-person screening technology development (FY 2019–FY 2022),
- AIT-1 & AIT-2 enhancement package deployment (FY 2020–FY 2021), and
- Next-generation on-person screening technology testing (FY 2022–FY 2024).

[18] O&S funding includes maintenance and federal payroll costs. Maintenance accounts for 94 percent of total O&S.

## Security Capability

AIT will continue to be a key component of passenger screening and is undergoing development efforts to enhance detection capabilities with more advanced threat detection algorithm software. TSA continues to explore the ability to conduct risk-based security by immediately changing detection algorithms and by using wideband algorithm integration to improve image processing and to address a variety of threats. TSA also is exploring the following capabilities:

- Adaptable/machine-learning algorithms, alternative millimeter wave frequency bands, passenger screening during continuous movement through the checkpoint, and the use of advanced imaging antennas to improve image processing and to identify a wider variety of threats. Adaptable algorithms and an open architecture would provide TSA with the flexibility to continue to enhance threat detection capabilities without replacing an entire machine.

- Enhanced AIT, which would allow for expedited clearing of alarms through multiple resolution screens, decreasing the bottleneck in passenger flow at the checkpoint.

- Flat panel screening technology used before the checkpoint, which can help to determine high-risk versus low-risk screening priorities. The use of flat panel technology could decrease the demand for primary AIT assets, thereby decreasing the footprint in screening areas.

- Algorithm integration and wideband development to advance the detection standard in the current and future fleet of AITs. The next generation of passenger screening technology will offer enhanced image resolution[19] by using a wider frequency bandwidth that supports more advanced algorithms for automated threat recognition detection.

## Interdependencies/Related Investment

TSA is conducting formal testing on its planned approach to connect these units to the STIP network before beginning operational testing later this year. Connectivity to STIP will provide a vehicle for obtaining metrics from the AIT and eventually will allow centrally controlled configuration. As the metrics currently require manual data entry from TSOs and others in the field, connectivity with STIP will provide TSA with increased data accuracy and availability. It also will reduce significantly the manual effort required to collect operational data and to monitor and maintain the TSE fleet. STIP connectivity also will result in faster and less costly deployment of software configuration changes, which will be important in a machine learning-enabled environment.

## Research and Development[20]

Analysis of TSA's current on-person screening capabilities validated the need to pursue R&D to enhance existing and next-generation systems to close the capability gaps. TSA and U.S.

---

[19] Images would not be viewable by a TSO operator.
[20] R&D efforts are focused on future on-person screening capability.

Department of Homeland Security (DHS) 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[21] by using a wider frequency bandwidth that supports more advanced algorithms for automated threat recognition detection.

Other R&D initiatives include adaptable/machine-learning algorithms, alternative millimeter wave frequency bands, "walk-through" screening capabilities for passengers, and the use of advanced imaging antennas to improve image processing and to identify a wider variety of threats. An open system architecture and adaptable algorithms will enable the flexibility to enhance threat detection through software updates and modular upgrades without the need to replace entire AIT systems.

TSA has developed enhancement packages for AIT-1 and 2 systems, which are in testing, with deployment scheduled for FY 2020, dependent on funding. The capabilities in these packages, including sensitive area box, targeted threat algorithm, clear queuing, and dynamic switching, provide a more focused threat detection capability while providing the operator with tools to maintain throughput. TSA also is exploring the use of multiple resolution screens for AIT that will expedite alarm clearance and will reduce bottlenecks in passenger flow at the checkpoint.

**Funding Profile**

The estimate in Figure A4 includes the sustainment cost for the existing AIT fleet and associated program overhead. Enhancement costs include the development, testing, and deployment of an improvement in detection capability and corrective actions.

***Figure A4: AIT, FY 2021–FY 2025***

| AIT – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$24.1** | **$23.8** | **$17.4** | **$19.4** | **$22.6** |
| **Total R&D** | **$5.0** | **$5.0** | **$12.7** | **$9.8** | **$7.5** |
| **Total** | **$29.1** | **$28.8** | **$30.1** | **$29.2** | **$30.1** |

# E. Advanced Technology X-Ray

**Overview**

Our current checkpoint X-ray system, AT, identifies and detects threats concealed in passengers' accessible property as they enter the screening checkpoint. AT systems are the primary technology for screening accessible property at screening checkpoints. Currently 2,234 AT units are deployed at approximately 430 airports nationwide.

***Illustration of AT X-Ray***

[21] Images would not be viewable by a TSO.

Automated screening lanes (ASL) are a property-handling system integrated into an existing AT to mitigate checkpoint security vulnerabilities, to improve checkpoint efficiency and throughput, and to reduce the number of misdirected bags identified for additional screening. TSA has partnered with airlines and airports to install ASL units at high-traffic security screening checkpoints and to connect them to existing AT systems. As of December 2019, TSA has deployed 184 ASLs to 16 airports and plans to install 12 additional units.

**Objectives and Goals**

The AT program's primary objective is to continue to enhance and automate threat detection at checkpoints. The AT program has primary planned milestones for deploying four enhanced threat detection capabilities between FY 2020 and FY 2025, dependent on availability of funds.

**Security Capability**

TSA uses AT X-ray systems at the checkpoints to screen roughly 3 million carry-on bags for explosives each day. AT X-rays detect threats in carry-on baggage by providing detection capability and two-dimensional visual screening of the contents in carry-on bags. Threat object discrimination has continued to improve through R&D efforts but comes at a cost of maintaining throughput efficiency and minimizing false-alarm rates.

As threats emerge and technical capabilities improve, enhancements to the AT X-ray systems at airports may include both software upgrades and procedural changes. TSA continues to work with vendors to develop and deploy enhanced detection capabilities. Newly identified threats may elude the current threat detection algorithms on the AT systems, so TSA needs the ability to address these threats quickly.

In FY 2019, TSA initiated deployment of enhanced algorithms that enable the detection of smaller quantities and an expanded library of explosive threats. These algorithms alert TSOs to potential threats in carry-on bags, therefore increasing the TSO's ability and efficiency to find prohibited items and ensuring greater consistency of applying resolution protocols. Over the coming fiscal years, TSA will replace most of these AT units on a one-for-one basis with newly procured CT/CPSS units. TSA will continue to deploy enhanced algorithm capabilities to address emerging threats.

**Interdependencies/Related Investment**

TSA has integrated and deployed 184 ATs and ASLs in the field. ASL is an enhancement to carry-on baggage scanners to automate bin return, tracking, and diverting to allow TSOs to perform critical security screening-related activities and to reduce passenger queue time. TSA is accepting ASLs under the Capability Acceptance Process and continues to work with ASL and AT system providers to incorporate new capabilities as part of these integrated systems.

**Desired Future Capabilities**

TSA continues to seek ways to enhance the security capabilities of its AT systems. TSA must continue to enhance detection capability of AT systems to meet emerging threats and to enhance capabilities to improve operational efficiency, including through X-ray imaging system enhancements, advanced algorithm development, stream of commerce false-alarm reduction, and threat characterization.

**Funding Profile**

The estimate in Figure A5 includes sustainment costs for the existing AT fleet and associated program overhead. Enhancement costs include developing, testing, and deploying improvements in AT detection capability and corrective actions. The table also includes costs for program support, maintenance and repair of gifted ASLs, and testing the ongoing interoperability of the ASL units with AT systems.

***Figure A5: AT, FY 2021–FY 2025***

| Advanced Technology X-Ray – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S[22][23]** | **$94.9** | **$100.0** | **$131.2** | **$134.3** | **$136.9** |
| **Total** | **$94.9** | **$100.0** | **$131.2** | **$134.3** | **$136.9** |

## F. Alarm Resolution Capability

**Overview**

The most commonly used alarm resolution capability is the ETD system, which detects trace amounts of explosive materials on passengers and their accessible property at the screening checkpoint and checked baggage. ETD technology is highly sensitive, thereby enabling fast and accurate screening for trace explosive quantities on a variety of surfaces. This enhanced explosive detection sensitivity gives TSOs the ability to detect a wide range of explosives threats.

***Illustration of ETD***

**Objectives and Goals**

The ETD program's primary objective is to continue to enhance screening of explosive trace on passengers, their accessible property, and checked baggage. ETD has three primary planned milestones between FY 2020–FY 2025, dependent on availability of funds:

- Smiths and L3 Harris ETD advanced threat detection standard development and deployment (FY 2020–FY 2022),

[22] O&S funding includes maintenance and federal payroll costs. Maintenance accounts for 71 percent of total O&S.
[23] AT and CPSS/CT are currently listed under one investment. This will change in the new reporting cycle when the CPSS/CT and AT programs become separate investments.

- Smiths and L3 Harris ETD advanced threat detection standard development and deployment (FY 2020–FY 2023), and
- Alarm-resolution program standup – ADE – 2A (FY 2022 Q4).

**Security Capability**

TSOs need to be able to resolve alarms from the primary screening device (for example, AIT, AT), so pursuing R&D activities to develop technology that can close this capability gap is important.  One of the main capability areas that will benefit from enhancement is updated detection standards on all currently fielded units.  TSA is testing an ETD advanced threat detection standard and, pending certification, plans to upgrade all ETD units in the field to this standard.  Investment in and deployment of future detection standards onto the currently fielded ETD fleet is dependent on the successful deployment of advanced threat detection standards.

In addition to advanced threat detection standards, TSA will update current ETD capabilities under the new Alarm Resolution Program, increasing the types and decreasing the quantities of detectable threats, and incorporating new cybersecurity requirements that will enable STIP connectivity.  TSA will incorporate these enhancements when the current fleet is recapitalized fully beginning in FY 2025.

**Interdependencies/Related Investment**

TSA is planning to connect the entire fleet of next-generation alarm-resolution technology to STIP, which will provide integration, solution deployment, endpoint cyber security solution and deployment, business intelligence tool and integration, and ongoing enhancement.

**Research and Development**

All current improvements to the ETD concept require direct access to the threat material in question or the presence of trace contamination on the outside of a container or concealment.  Further R&D will enhance the capability to detect and identify threat materials that are in a container or other concealment that cannot be opened or sampled.  Future investments in R&D are focused on noncontact trace sampling, high-resolution ETD systems, and vapor detection systems.

**Funding Profile**

The estimate in Figure A6 includes sustainment costs for the existing ETD fleet and associated program overhead.  Enhancement costs include development, testing, and deployment of improvements in detection capability and corrective actions.

*Figure A6: Alarm-Resolution Capability, FY 2021–FY 2025*

| Alarm Resolution Capability –FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
| Total O&S[24] | $23.8 | $23.5 | $24.1 | $24.0 | $24.8 |
| Total R&D | $3.0 | $3.0 | $13.8 | $4.9 | - |
| ETD Total | $26.8 | $26.5 | $37.9 | $28.9 | $24.8 |

## G. Passenger Screening Program Legacy

### Overview

The Passenger Screening Program (PSP) Legacy fields, sustains, maintains, and disposes of the capabilities necessary to detect threats concealed on passengers and their accessible property as they enter the screening checkpoint. The systems within the PSP Legacy portfolio provide primary and secondary screening capabilities for the checkpoint while new technologies are being developed to detect ever-evolving threats better. Current legacy technologies include the following:

- **Bottled Liquid Scanners (BLS):** Differentiates dangerous liquids and compounds from common, benign substances carried by passengers during the checkpoint screening process in clear bottles.

- **Boarding Pass Scanner (BPS):** Reads a passenger's boarding pass and displays the passenger's name, flight information, and risk status to the TDC.

- **Chemical Analysis Devices (CAD):** Screens unknown liquid and solid (including powder) materials.

- **Enhanced Metal Detectors (EMD):** Detects potentially dangerous metallic threats and promotes high passenger throughput capabilities, allowing for the rapid inspection of passengers in transit.

### Objectives and Goals

PSP Legacy's top priority is to field, maintain, sustain, and dispose of legacy capabilities within the checkpoint. In addition, the program aims to meet current and new detection standards, to integrate and streamline technology processes further, and to enhance collaboration and engagement with stakeholders. PSP Legacy has several key milestones planned for FY 2020–FY 2025 across its portfolio of technologies, dependent on availability of funds:

[24] O&S funding includes maintenance and federal payroll costs. Maintenance accounts for 75 percent of total O&S through FY 2022. FY 2023–FY 2025 includes O&S costs that reside with TSA's Requirements and Capabilities Analysis (RCA) for alarm resolution. The percentage of maintenance will vary on the basis of the procurement and deployment schedule.

**BLS:**

- FY 2020-FY 2023:  Procure new units in support of airport expansion
- FY 2023-FY 2025:  Begin transitioning BLS to future Alarm Resolution Program

**BPS**:

- FY 2020–FY 2024:  Procure new units in support of airport expansion
- FY 2020–FY 2024:  Begin transitioning BPS to CAT

**CAD**:

- FY 2023–FY2025:  Begin transitioning CAD to future Alarm Resolution Program

**EMD**:

- FY 2020–FY2024:  Procure new units in support of airport expansion

**Security Capability**

The PSP Legacy program is in the sustainment phase of the acquisition lifecycle.  As such, the fleet of PSP Legacy systems will remain fielded until new capabilities replace the systems.

**Interdependencies/Related Investment**

As part of the technology enhancement process, TSA is working to connect enhanced metal detectors to STIP to automate nonsecurity functions, to support remote centralized configuration management, and to enhance data collection.

**Funding Profile**

Figure A7 includes sustainment costs for existing BLS, BPS, CAD, and EMD systems and the associated program overhead costs.

***Figure A7:  PSP Legacy, FY 2021–FY 2025***

| Passenger Screening Program (PSP) Legacy–FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
| Total O&S[25] | $10.3 | $12.4 | $12.3 | $12.3 | $12.7 |
| Total | $10.3 | $12.4 | $12.3 | $12.3 | $12.7 |

[25] O&S funding includes maintenance and federal payroll costs.  Maintenance accounts for 25 percent of total O&S.

# II. Transportation Security Equipment Portfolio

As of September 2019, TSA manages 15,000 total deployed TSE across more than 440 airports.[26] However, TSA's focus is not on specific security equipment and technologies, but on meeting capability needs. Managing and planning for TSA's fleet of TSE requires significant consideration and balance between maintaining and recapitalizing existing equipment, purchasing and deploying equipment to close gaps between airports or to accommodate increased passenger volumes, and investing in and deploying equipment with new capabilities.

## TSE Useful Life and Recapitalization

Managing and maintaining TSA's fleet of TSE requires diligently monitoring existing equipment and planning for projected recapitalization needs. Figure A8 depicts the useful life of deployed TSE, the number of TSE deployed as of September 2019, and the number of airports fielding those TSE.

***Figure A8: Overview of Useful Life for Deployed TSE***

| Currently Deployed TSE | Projected Useful Life | # Deployed as of 9/30/19 | # Airports Deployed to as of 9/30/19[27] | # Estimated Deployed Past Useful Life[28] |
|---|---|---|---|---|
| **EDS** | 15 years | 1,681 | 286 | N/A[29] |
| **ETD[30]** | 10 years | 5,715 | 430 | 0 |
| **AIT** | 10 years | 952 | 337 | 3 |
| **AT** | 10 years | 2,230 | 430 | 1 |
| **BPS[31]** | N/A | 2,300 | 421 | -- |
| **BLS** | 10 years | 1,628 | 428 | 1 |
| **EMD** | 10 years | 1,371 | 430 | 507 |
| **CAT** | 10 years | 47 | 15 | 0 |

The useful life projections outlined in the table above are estimates.[32] TSA replaces TSE at the point of technological obsolescence, which occurs when TSE cannot be upgraded further to meet new detection standards. TSA plans to replace many of the technologies above with next-generation equipment to meet new capability needs. These projections, however, can change as TSA routinely inspects its deployed technology by analyzing maintenance data, including performance metrics and deployed fleet age information.

---

[26] The term "deployed" refers to TSE in active use, including items used for screening at all federalized airports, as well as units deployed to test facilities and training locations.
[27] TSE also may be deployed at additional sites, such as training and test facilities.
[28] Figures based on the 2019 Transportation Security Equipment Useful Life Analysis Report. Figures as of June 2019.
[29] Only EDS models defined as technically obsolete for inability to meet next detection standards are beyond their useful life. A system's age is not considered a determining factor of useful life for EDS.
[30] Includes ETD units from the Checkpoint Technologies Division and EBSP.
[31] BPS data are as of March 2015 because of tracking constraints.
[32] A full discussion of the methodology to arrive at useful life estimates is available on page 21 of the 2015 Plan.

This reliability, maintainability, and availability of data allow TSA to analyze actual performance in the field and to revalidate service life estimates annually. TSA also works with industry to identify efficient and innovative ways to extend the life of TSE. For example, all major components and operating systems of TSE now can be replaced upon failure, allowing TSE to remain in a high state of readiness without the need for calendar-driven recapitalization efforts.

## TSE Planned Purchases

Figure A9 depicts planned purchases for FY 2020 through FY 2025. FY 2020 data are based on TSA's FY 2020 enacted budget. For subsequent fiscal years, data are based on the latest available TSA program cost models. These cost models reflect TSA's initial responses to budgetary changes and are used to build lifecycle cost estimates (LCCE).

To determine long-term budget implications related to operations and support, and in accordance with DHS policy, TSA uses LCCEs for its acquisition programs to manage cost baselines and to balance affordability and requirement trade-offs. LCCEs undergo continuous revision as priorities and funding profiles change. Actual purchase quantities are based on available funding and changing realities of the security environment. TSA also may procure evaluation units of new commercial off-the-shelf TSE for demonstrations and developmental testing to assist in the development of future requirements.

***Figure A9: Approved Checkpoint Technologies Division (CTD) and EBSP Planned Procurements as of January 2020[33]***

| TSE | FOC | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
|---|---|---|---|---|---|---|---|
| **EDS[34]** | **---[35]** | **58** | **47** | **28** | **11** | **8** | **0** |
| **ETD[36]** | **5,860[37]** | **20** | **0** | **0** | **0** | **0** | **0** |
| **AIT** | **962** | **0** | **0** | **0** | **0** | **0** | **0** |
| **AT** | **2,213** | **0** | **0** | **0** | **0** | **0** | **0** |
| **BLS** | **1,530** | **0** | **0** | **0** | **0** | **0** | **0** |
| **CAT[38]** | **1,520** | **475** | **493** | **0** | **0** | **0** | **0** |

33 This table does not include quantities for potential airport expansion or future acquisition program procurements.
34 EDS planned procurement figures for FY 2020 are based on the approved operating plan; figures for FY 2021–FY 2025 are based on the FY 2019 annual update.
35 EBSP met initial FOC in 2003 upon deploying enough ETDs and EDSs to screen 100 percent of checked baggage. There are currently 1,670 EDSs deployed. Given the improved capabilities of new EDSs, such as throughput, and the extended useful life of EDSs (currently 15 years), total quantity of deployed EDSs fluctuates as operational conditions require.
36 Includes ETD units from CTD and EBSP.
37 This is a combined CTD/EBSP ETD count as they are a shared resource. There are 3,222 for CTD and 2,638 for EBSP.
38 The CAT units are not recapitalizations because no units currently are deployed, but they are planned purchases for an existing program. The quantity of and fiscal year in which the CAT units are to be purchased are subject to change as TSA is performing developmental testing on CAT.

| TSE | FOC | FY 2020 | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
|---|---|---|---|---|---|---|---|
| **CPSS** | **2,181**[39] | **0** | **161**Error! Bookmark not defined. **40** | **TBD**[40] | **TBD**[402] | **TBD**[402] | **TBD**[402] |
| **EMD** | **960** | **0** | **0** | **0** | **0** | **0** | **0** |
| **BPS**[41] | **---** | **0** | **0** | **0** | **0** | **0** | **0** |

The information above is notional and subject to approved funding. It is not intended to communicate confirmed planned procurements because these programs may evolve along with the capability areas described above, and are shown to provide insight into TSA's strategic direction. Additionally, each capability must meet TSA and DHS requirements.

[39] CPSS FOC is based on the assumption that there will be a one-to-one replacement of ATs with CPSSs.
[40] Quantities for FY 2022, FY 2023, FY 2024, and FY 2025 will be determined by the CPSS Program Strategy, available funding, and vendor readiness.
[41] During development of the 2015 5-Year Strategic Plan of Investments report, BPS was not considered a separate project within the PSP; instead, requirements and funding were reflected under the CAT project in the PSP LCCE and Acquisition Program Baseline documentation.

# III. Other Capital Investments

## A. Future Lane Experience Screening

TSA aims to build upon its existing model of passenger prescreening, identity verification, and checkpoint screening to differentiate physical screening further on the basis of risk with FLEx and the introduction of biometrics technology at the TSA checkpoint.

FLEx aims to improve security effectiveness and operational efficiency by further differentiating passengers by risk and by offering modified screening tailored to these new risk designations. The first phase of this effort will be to differentiate the expedited screening population and to reassess the appropriate level of screening required for entry into the sterile area. TSA will modify Secure Flight vetting to return an increased number of vetting results, including a new low-risk status. The further differentiation provided by FLEx will result in increased security in the airport environment.

## B. Secure Flight

**Overview**

Secure Flight identifies the appropriate level of physical screening for all passengers and minimizes misidentification of individuals. Secure Flight operates a threat-based watchlist and Trusted Traveler-matching capabilities that 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. Secure Flight matching uses the Federal Bureau of Investigation's Terrorist Screening Database to identify known or suspected threats to aviation security. TSA also partners with other DHS Components to identify potential threats to aviation security that are not listed in the Terrorist Screening Database and partners with U.S. Customs and Border Protection (CBP) to identify Trusted Travelers.

**Security Capability**

Today, TSA segments passengers into four risk tiers: TSA Pre✓®, standard, selectee, and no-fly. FLEx will add further differentiation within this standard risk tier. Further vetting and preflight risk analysis to drive risk differentiation and operational activities (including Federal Air Marshal information sharing) will increase screening effectiveness for higher-risk passengers. In addition, Secure Flight will operate with CAT to identify where the name screened by Secure Flight does not match the boarding pass and/or passenger identity or travel document presented at checkpoints. This will enable real-time Secure Flight updates, significantly enhancing security. TSA's ability to prescreen and vet risk functionality requires adaptability with the evolving threat to aviation security. Enhanced risk capability:

- Reduces the potential security vulnerability of known or suspected terrorists circumventing TSA's vetting processes,

- Assists in mitigating the effects from increased passenger travel volume,
- 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 better compared to watchlist information and to increase automation to identify potential higher risk passengers better, and
- Informs operations and resource planning.

Improved vetting and identity verification, including implementing real-time feedback from passenger encounters (for example, known or suspected terrorist screening results) to TSA screening and vetting systems along with using biometrics technology at checkpoints, will increase screening effectiveness and improve security.

TSA requires investment to enhance the segmenting of Secure Flight passengers on the basis of risk and encounter information capabilities in the current threat environment to ensure aviation security and to protect the homeland against terrorist acts. This investment includes required changes in name-matching algorithms and vetting adjustments to incorporate additional risk factors beyond direct watchlist and Trusted Traveler matching. These changes will result in a more automated engine that improves high-risk passenger rules and watchlist matches while significantly decreasing false positives and minimizing risk for potential false negatives. This maturation of the system and operations would include built-in, real-time data analytics capability to drive operational planning and responses and to provide feedback to the intelligence community. It also would provide a platform for real-time reporting and metrics of passenger information across the aviation system.

Enhanced capabilities for Secure Flight matching and risk segmentation will enable vetting analysts to review and respond rapidly using existing resources while travel volumes continue to increase. These changes will create more effective prescreening and allow TSA to provide the required advanced notice to field screening and the law enforcement/Federal Air Marshal Service operation to drive and inform their scheduling and security activities better. These changes also will continue to mitigate concerns that adversaries might take advantage of potential security vulnerabilities because of delayed identification and notification to the field. Additionally, enhanced Secure Flight capabilities are critical for routing new vetting status designations and implementing FLEx screening.

**Interdependencies/Related Investments**

Identity management underpins our vetting effectiveness. Currently, TSA communicates a limited range of vetting statuses (TSA Pre✓®, standard, and selectee) to the checkpoint via the airline boarding pass. Communicating even these few tiers with higher confidence—and especially any further segmentation as described above—requires the ability to communicate directly between Secure Flight and the checkpoint. CAT units will enable that direct communication and will increase TSA's ability to act on improved vetting and credentialing.

As biometric identity verification comes online, Secure Flight will be even more critical as a data source for checkpoint operations. Biometrics hold promise for achieving significant savings by

allowing retasking of TSOs currently needed to screen travel documents, increasing confidence in passenger identity, and enabling mostly automated lanes for screening known travelers. Further, passing biometric data from central data centers to checkpoint security equipment will require the cyber-secure networking of these sensitive data that STIP is developing. Investments in these areas are interdependent, and many screening improvements will be less effective if Secure Flight does not receive the investment necessary to handle the back-end vetting that underpins risk-based screening.

**Funding Profile**

TSA plans to develop and implement vetting risk segmentation capabilities first, in conjunction with FLEx and then an end-to-end encounter data capability. This capability is needed to share real-time encounter information to enhance high-risk passenger identification in vetting, particularly related to selectee screening with FLEx. Additionally, a portion of funding each year as shown in Figure A10 will be used for continued operations of interfaces and equipment maintenance.

***Figure A10: Secure Flight, FY 2021–FY 2025***

| Secure Flight – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
| Total O&S | $117.9 | $121.6 | $106.5 | $107.6 | $109.3 |
| Total | $117.9 | $121.6 | $106.5 | $107.6 | $109.3 |

# C. Biometrics Technology

**Overview**

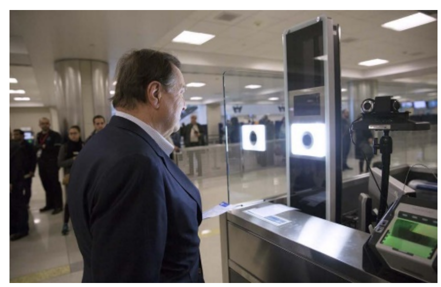


***Illustration of Biometrics capability***

In April 2018, CBP and TSA signed *The Joint TSA-CBP Policy on Use of Biometrics*, committing to exploring the use of biometric facial recognition technology. In October 2018, TSA published its Biometrics Roadmap that articulates an approach for TSA to use biometrics technology to increase security effectiveness while also improving operational efficiency and the passenger experience. To support this vision, the roadmap outlines four strategic goals that TSA will pursue to deploy biometric facial recognition technology in the field:

- Partner with CBP on use of biometric identification technology for international travelers at TSA security screening checkpoints,
- Operationalize biometrics for identity verification of TSA Pre✓® travelers,
- Expand biometric identification technology to additional domestic travelers, and
- Develop supporting infrastructure for biometric solutions.

To foster collaborative partnerships and to develop a coordinated strategy, the TSA Biometrics Roadmap incorporated feedback gathered during more than 40 targeted engagements with

aviation security leaders from airlines, airports, and solution providers. Airlines and airports have expressed a strong interest in streamlining and modernizing the passenger experience and in using biometrics technology in their own business processes.

The roadmap articulates a collaborative biometric vision for TSA and its aviation security partners in the context of an overall identity verification and management approach. It also highlights facial recognition technology as the preliminary method of choice, to align with partners and current processes for manual facial matching. The roadmap also acknowledges that multimodal approaches may help to increase further the accuracy, security, and scalability of TSA biometric operations over time. TSA continues to refine and execute the strategy outlined in the roadmap to leverage biometrics to enhance security effectiveness, to increase efficiency, and to improve the passenger experience.

To enable future pilot efforts and a long-term biometric solution, TSA is planning and executing capability analysis and development efforts to support deployment of this technology in the field, and to ensure the confidentiality, security, integrity, and availability of biometrics data. From an architecture perspective, this includes developing a solution that uses existing and evolving TSA infrastructure, while also identifying and investing in key systems integration activities to support a future state solution.

Additionally, TSA is working with interagency and industry partners to identify and address potential privacy or performance bias issues associated with biometrics technology, in compliance with the TSA Modernization Act of 2018. Finally, TSA is working to build consistent, testable requirements and to develop procurement and acquisition strategies for future deployment. These activities will allow TSA to enable the development of a viable biometric solution for the aviation sector, focusing initially on TSA Pre✓® and other Trusted Travelers for both domestic and international flights.

**Security Capability**

In 2018, TSA's Transportation Security Capability Analysis Process (TSCAP) analyzed its current ability to perform identity verification. The results of this analysis validated the need to pursue biometrics technology to improve capabilities. The desired end-state is one in which appropriate TDC functions are automated via biometrics because biometrics technology could validate passenger identity and vetting status more effectively and efficiently than can the current manual processes.

To close capability gaps and to achieve TSA's future state goals associated with security, effectiveness, and passenger experience, TSA requires the ability to develop, procure, and deploy a capability to allow biometric verification of passenger identity and to confirm passenger vetting status in real-time. By developing an architecture that supports the automation of TDC functions, TSA can control access to the sterile environment better, can improve the traveler experience, and can reallocate resources to realize screening efficiencies.

**Interdependencies/Related Investment**

Deployment and use of biometrics technology will depend on the deployment of CAT and STIP. This approach maximizes the investment that TSA already has made in existing mission architecture to operationalize risk information at the checkpoint. TSA is working with CBP on a biometrics architecture to enable and facilitate TSA's biometrics-based identity verification capability at the checkpoint. The system integration with CAT and STIP also will facilitate linking the front-end hardware to internal and external networks, including CBP, DHS's Office of Biometric Identity Management, and Secure Flight.

**Research and Development**

The R&D costs would include STIP interface development activities to build back-end business integration and biometric storage capabilities. Third-party technology development will be necessary to determine the appropriate governance and infrastructure to support non-TSA-owned biometric technologies outside the TDC. In addition, implementation of biometrics technology will require R&D for systems integration, biometric system improvements, data analytics and algorithm development, cybersecurity, and standardization and requirements.

**Funding Profile**

The funding values in Figure A11 are based on a biometrics system catering to TSA Pre✓® passengers. However, additional functionality to increase operational efficiencies for screening other traveling populations will increase unit costs.

***Figure A11: Biometrics Technology, FY 2021–FY 2025***

| Biometrics Technology – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | FY 2021 | FY 2022 | FY 2023 | FY 2024 | FY 2025 |
| Total O&S | $2.0 | $2.0 | $5.0 | $5.0 | $5.0 |
| Total | $2.0 | $2.0 | $5.0 | $5.0 | $5.0 |

## D. Automated Exit Lanes

**Overview**

Exit lane breaches introduce risk to passengers and aircraft, but resolving these breaches is costly and highly disruptive. Because of resource constraints, TSA does not qualify, procure, or maintain exit lane technologies. Instead, TSA provides a set of web-based, self-guided tools for airport use in identifying technologies for exit lane access control and evaluating systems for installed exit lane technology.

***Image of Automated Exit Lanes***

The TSA Modernization Act of 2018 authorized TSA to establish partnerships with small airports and to start a pilot program to enhance their ability to

use technology better to protect exit lanes, with an interest in expanding pilot programs to larger airports. Although funding was authorized, no funds were appropriated. TSA partially met the intent of the legislation by selecting pilot participants using a risk-based methodology and by collecting data on that airport's use of advanced exit lanes security technology.

**Security Capability**

At large airports across the system, exit lane controls primarily are built around an in-person TSO, security guard, or law enforcement officer responsible for monitoring the lane for unauthorized entry. Introducing technology as an exit lane control allows for better use of TSA and airport security staffing against other system risks because it reduces the potential for human error in this function and better invests trained personnel in skilled checkpoint functions.

**Interdependencies/Related Investment**

Automated Exit Lanes is a standalone pilot program authorized, but not appropriated, under the TSA Modernization Act of 2018. TSA is responsible for monitoring 262 co-located exit lanes at 117 airports, which are staffed by 1,457 TSOs. Through automation of exit lane monitoring, TSA could free up trained officer resources to conduct security measures at checkpoint lanes and in baggage rooms.

## E. Checkpoint Wait Times

**Overview**

The TSA Modernization Act of 2018 tasks TSA with establishing a system that captures checkpoint wait times in real-time from the beginning of the queue through the end of the security process, that implements physical displays of wait times to passengers, and that establishes a location online where wait times are displayed in real-time. TSA plans to collaborate with the airport industry and technology vendors to develop performance-based guidelines and tools that airports can use to evaluate, assess, and plan their technology investments for crowd movement. To date, TSA has completed two demonstrations of technology solutions capable of fulfilling the statutory requirements, has released an information request on the technologies available in the industry, and has planned to install a proof-of-concept during the first quarter of FY 2020.

**Security Capability**

Crowd movement technologies in the industry can do more than collect passenger wait time data. Additional data captured from this process has the potential to help TSA to operate more efficiently and effectively in terms of allocating staff, scheduling TSOs, opening screening lanes, and managing checkpoint operations. Implementing wait-time reporting systems across airports also has the potential to increase security, to reduce wait times, to increase transparency, and to improve stakeholder relationships.

## F. National Explosive Detection Canine Team

### Overview

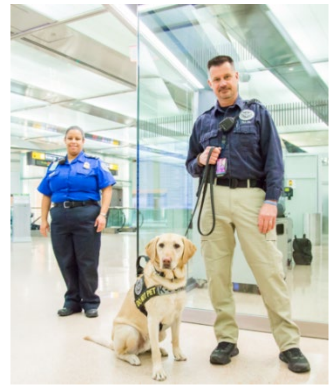


***Illustration of National Explosives Detection Canine Team***

Canine teams from the National Explosive Detection Canine Team Program (NEDCTP) deter and detect the introduction of explosive devices into the transportation system. NEDCTP is a partnership in which airports, mass transit, and maritime transportation systems voluntarily participate. TSA trains both federal (TSA-led) and nonfederal (state and local law enforcement-led) canine teams to protect transportation systems against terrorist attacks. TSA has deployed passenger screening canine (PSC) teams since 2011. These teams are vital to TSA's risk-based security initiatives given their ability to detect explosives concealed on the body or in a passenger's accessible property.

This program has grown significantly in the past several years because of its proven effectiveness and reliability as a mobile security screening resource. Program scope includes 1,097 authorized explosives detection canine teams at more than 100 of the Nation's airports, mass transit, and maritime systems. State and local law enforcement partners lead 675 teams; TSA handlers lead 422.

Recently, TSA opened the opportunity for qualified explosives detection canine teams and canine team providers to become a registered certified cargo screening facility-canine under TSA's Certified Cargo Screening Program-Canine. This program fulfills a requirement in the TSA Modernization Act of 2018 to develop standards for the use of third-party canines for air cargo screening and allows TSA to expand its network of certified screening canines to enhance aviation security.

### Security Capability

Rising passenger volumes and soft-target attacks demonstrate the need to counter the threat of improvised explosive devices with a highly visible and effective deterrent such as PSC teams. PSC teams, combined with canine enhanced screening, have proven to decrease wait times, which reduces the number of passengers accumulating at the checkpoint area; thereby reducing the risk that the security checkpoint would become an attractive target for a terrorist attack. FLEx enables a more efficient and effective working environment for the canines because FLEx will drive risk differentiation, allowing canines to focus on the true unknown population.

Although TSA has focused PSC teams on checkpoints, they are also a highly mobile asset that can be deployed quickly throughout the airport or other transportation environments to address a variety of emerging threats. They are an effective alternative resource to screening areas that have an explosives-based risk but are not conducive to traditional screening technologies. When necessary, PSC teams can be used to sweep terminals, cargo warehouses, or other transportation facilities. In addition, they can be used in airport secure areas to combat insider threat operations or to respond to large-area, large-volume events such as system malfunctions in electronic

baggage screening.  PSC teams also can be an invaluable asset away from the airport environment at locations such as train stations, mass transit hubs, ferry terminals, and national special security events.

**Research and Development**

TSA continues to partner with DHS S&T for R&D activities that may advance or validate canine explosives detection capabilities on the basis of DHS S&T's responsibility as the central focal point for DHS canine research, development, test, and evaluation.  DHS S&T focuses on developing and testing canine training aids that can be used to improve and test canine ability to detect new threats, independent operational test and evaluation (T&E) capability for detection canines, and canine R&D structure and function to improve operational efficiencies and training methods.

**Funding Profile**

***Figure A12:  TSA Led NEDCTP, FY 2021–FY 2025***

| TSA-Led Explosives Detection Canine Team – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$135.9** | **$136.3** | **$136.4** | **$137.8** | **$140.1** |
| **Total** | **$135.9** | **$136.3** | **$136.4** | **$137.8** | **$140.1** |

***Figure A13:  State and Local Law Enforcement Explosives Detection Canine Team Program, FY 2021–FY 2025***

| State and Local Law Enforcement Explosives Detection Canine Team – FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$34.8** | **$34.8** | **$34.8** | **$34.8** | **$34.8** |
| **Total** | **$34.8** | **$34.8** | **$34.8** | **$34.8** | **$34.8** |

## G. Countering Unmanned Aircraft Systems

**Overview**

DHS received limited authorities to counter unmanned aircraft systems (UAS) threats in the Preventing Emerging Threats Act of 2018, which passed with bipartisan support as part of the 2018 Federal Aviation Administration (FAA) Reauthorization Act.  DHS is working to implement these authorities in coordination with FAA.  To support DHS efforts, TSA is developing appropriate security measures and responses to counter threats from UASs in the airport environment.

TSA is leading an interagency effort to develop a unified plan for responding to a persistent disruption of air traffic operations caused by unauthorized UASs.  This plan provides an immediate, effective response to incidents, while the National Strategy for Aviation Security develops and reinforces more comprehensive, end-to-end strategies.  TSA developed the *Unified National Level Response to Persistent UAS Disruption of Operations at Core 30 Airports* concept of operations (CONOPS) in October 2019.  Deputies from U.S. Government

departments and agencies approved the CONOPS, which designates TSA as the lead federal agency for a unified national-level response to a persistent UAS disruption at a Core 30 airport and outlines how TSA will fulfill that role.

TSA is working with airport authorities, federal security directors, and other key stakeholders to develop a risk-based, nationally consistent, and harmonized tactical response plan for UAS airport incidents. The responses must be supported by proven and tested technologies while safely limiting effects on aviation operations. This requires multiple threat and vulnerability assessments, the development of operational and technical requirements, field testing, and the development and execution of counter-UAS (C-UAS) training.

TSA incrementally is developing the capability to identify technology systems that detect, identify, track, and mitigate UAS threats in the airport environment. To verify and validate UAS equipment most suitable for an airport environment, TSA is leading efforts to establish UAS technology test beds so that TSA can test detection equipment and eventually can test C-UAS equipment to keep up with the rapidly evolving technology marketplace and emerging threats. TSA also plans to conduct UAS-focused joint vulnerability assessments at certain airports, to deliver operational training for C-UAS technologies in the field, and to manage C-UAS security policies, plans, and engagement for aviation, surface, and other transportation domains.

**Security Capability**

As the designated lead federal agency for responding to persistent UAS-related incidents at airports, as defined by the CONOPS, TSA must remain ahead of the adversary by clearly understanding the threat, vulnerabilities, and potential countermeasure systems. The number of encounters with UASs around airports and with civil aircraft has increased over the years as UASs proliferate. Additionally, 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 lack of federal capabilities, many airport authorities independently are acquiring their own UAS detection and mitigation systems. However, without centralized federal guidance, this potentially poses more danger at airports and results in operational and procurement inefficiencies with the deployment of disparate systems.

**Funding Profile**

This budget as shown in Figure A14 heavily leverages cost-sharing partnerships with public and private entities to be as effective as possible across 450+ airports. Additionally, this budget considers cost savings over time through efficiencies.

***Figure A14: Countering Unmanned Aircraft Systems, FY 2021-FY 2025***

| **Countering Unmanned Aircraft Systems – FYHSP Constrained FY 2021–FY 2025 ($M)** | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$3.0** | **$8.2** | **$19.7** | **$19.8** | **$18.5** |
| **Total** | **$3.0** | **$8.2** | **$19.7** | **$19.8** | **$18.5** |

## H. Air Cargo

**Overview**

TSA must screen 100 percent of cargo transported on passenger aircraft at a level of security equal with the level of security for the screening of passengers' checked baggage. TSA regulates cargo screening technologies through the air cargo screening technology list. It includes more than 110 technology systems, all of which are regulated in terms of both hardware and software. Any changes to a system's configuration must be assessed and potentially must be tested in the lab and field to ensure that no vulnerabilities occur when systems are changed or upgraded. More stringent detection standards have caused many CT and ETD systems currently available for air cargo screening to become outdated, requiring them to be removed incrementally. To meet the new TSA detection standards, most systems will have to be modernized or completely replaced over the next 5 to 10 years.

**Security Capability**

The TSA Modernization Act of 2018 requires TSA to initiate a 2-year pilot program to achieve enhanced air cargo security screening outcomes using new screening technologies, such as CT. No funding was appropriated for this pilot program, and TSA has not allocated any additional funding to the air cargo technology program for this purpose. Despite the lack of funding, TSA is trying to meet as many Modernization Act objectives as possible through planned and scheduled field assessments of EDS in collaboration with an industry partner.

Currently, only one field assessment is scheduled. As additional systems move through the qualification process and fully meet requirements, industry partners with which TSA already has formal test bed relationships will be contacted regarding their interests in participating in further EDS operational assessments. These emerging technologies would replace existing capabilities to meet new TSA standards.

**Funding Profile**

The funding detailed in Figure A15 covers the costs associated with air cargo security screening.

***Figure A15: Air Cargo, FY 2021-FY 2025***

| Air Cargo – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$15.2** | **$15.4** | **$15.4** | **$15.4** | **$15.4** |
| **Total** | **$15.2** | **$15.4** | **$15.4** | **$15.4** | **$15.4** |

# I. Security Technology Integration Program

**Overview**

STIP is focused on the automated exchange of information from TSA and enhancing the capability to connect TSE to a TSA network while securing them from cyber threats. STIP addresses the following key capability gaps:

- **Security:** TSA lacks the capability to transfer information dynamically between TSE and vetting and security operations information.
- **Configuration Management:** TSA lacks the capability to upload configuration updates and software on TSE automatically, as well as the capability to collect, track, and harmonize configuration settings efficiently.
- **Information Sharing and Enterprise Management:** TSA lacks the capability to automate data collection processes used to capture and upload operational data from TSE.
- **Resource Management:** TSA lacks the capability to collect TSO threat detection performance data from TSE automatically.

Once TSE is connected to a network, STIP could monitor, diagnose, troubleshoot, and manage TSE remotely, allowing TSA to address equipment issues and prevent failures.

**Security Capability**

TSA's path forward is to provide support for checkpoint equipment to allow for the integration of security screening technologies into the STIP platform. Enhancements to the STIP platform also will support new capabilities that are demonstrated or deployed to the field, such as emerging biometrics technology efforts.

**Interdependencies/Related Investment**

STIP functionality will be developed in coordination with TSE that will use STIP to connect their systems to the TSA network. Future capabilities will be developed to integrate with STIP to:

- Define and support secure standardized interfaces to collect TSE operational and asset management data from the checkpoint and checked baggage,
- Provide the connectivity required to transmit maintenance and enhancement releases securely for TSE application software and firmware,
- Collect airport incident and investigation data, and

- Support the analysis and reporting of airport operational, incident, investigation, and asset management data, including support for airport operations centers.

Before connecting to STIP, TSE will need to have automated interfaces, which involves collecting and formatting the operational and asset management data for reporting, as well as receiving and applying software releases. Some programs also will need to modernize the operating systems and application code running on the TSE to meet current cybersecurity standards.

**Desired Future Capabilities**

As TSA begins to develop and deploy machine-learning algorithms and advanced system data analytics and visualization capabilities, the need for updated computing and data architecture elements must be addressed. 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.

**Funding Profile**

In Figure A16, TSA is maintaining STIP connectivity for CAT, AIT, and EMD units, as well as manual data collection capability for the rest of the TSE fleet. TSA also requires funding to deploy and maintain the STIP solution for legacy TSE.

***Figure A16: STIP, FY 2021–FY 2025***

| STIP – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$12.3** | **$13.9** | **$12.7** | **$12.9** | **$13.2** |
| **Total ($M)** | **$12.3** | **$13.9** | **$12.7** | **$12.9** | **$13.2** |

# J. Information Technology Infrastructure Program

**Overview**

The Information Technology Infrastructure Program (ITIP) provides modern information technology (IT) services to support TSA in the execution of its overall national security mission. IT services and associated infrastructure are required to meet the basic computing and communications needs while sustaining maintenance for the TSA user community. This basic requirement has expanded because of the addition of intermodal requirements (rail, highway, transit, maritime, pipeline, and infrastructure) requiring core IT infrastructure augmentation and enhancements. These mission-essential demands have obligated TSA to sustain increasing services, contracts, and indirect costs associated with TSA's complex hosting environments.

ITIP manages the operations and maintenance of IT infrastructure to ensure uninterrupted operational availability of IT services (operations, engineering, end-user services, application development, information assurance, enterprise architecture, and mission support) required for

all business and mission needs. TSA's IT infrastructure greatly enhances the ability to collect data, to process data, and to transfer voice, video, or digital information to make informed decisions. TSA IT users and customers require basic modern IT tools such as computers, servers, databases, mobile devices, telephones, printers, and copiers to perform their daily work. The following initiatives each contain specific objectives to advance the program closer to the desired future state:

- **Cloud:** To reduce IT costs and to create a secure environment to host applications and infrastructure, TSA IT is migrating apps to cloud-based and hybrid environments. By reducing the infrastructure footprint, TSA will be able to reduce infrastructure maintenance and service costs as well as resource needs. The cloud transformation requires strategic planning that maps individual business capabilities to the most appropriate cloud-service model and platform. This will lead to improved productivity, greater accessibility and capacity, and increased flexibility for systems and processes.

- **IT Lifecycle Management:** Standardizing the annual refresh schedule for all equipment will allow TSA to refresh outdated hardware on a regular and predictable schedule, which will reduce the risk of equipment performance delays, recurring issues, and total failure. Performance is measured by the overall functionality of equipment, which directly affects the effectiveness of security staff, law enforcement, and TSOs who provide mission-essential services.

- **Operations and Maintenance (O&M):** The current infrastructure operations and maintenance program provides a wide range of IT professional services supporting a large and diverse technological environment. Because of an increasingly expensive and competitive IT and cyber industry, TSA is expecting an increase to the costs of its current O&M support model. TSA's objective is to ensure that future O&M support is funded to cover completely all necessary requirements for maintaining the enterprise services provided under ITIP.

- **Cybersecurity:** This investment will supplement TSA's current cybersecurity capabilities to address TSA's expanding IT infrastructure and to provide cybersecurity support for emerging programs without delaying the current cybersecurity support provided to TSA's 70+ FISMA systems.

**Funding Profile**

The following funding in Figure A17 will enable TSA to continue to provide IT equipment and services across TSA, providing technical support and enhancements of the information technology capabilities required by the agency's domestic and international workforce.

***Figure A17: ITIP, FY 2021-FY 2025***

| ITIP – FYHSP Constrained FY 2021–FY 2025 ($M) | | | | | |
|---|---|---|---|---|---|
| | **FY 2021** | **FY 2022** | **FY 2023** | **FY 2024** | **FY 2025** |
| **Total O&S** | **$357.0** | **$345.5** | **$345.5** | **$345.0** | **$345.0** |
| **Total** | **$357.0** | **$345.5** | **$345.5** | **$345.0** | **$345.0** |

# IV. Technology Investment Framework

In 2015, TSA introduced the Technology Investment Framework, a two-phase process consisting of the Pre-Need phase and the Acquisition Lifecycle phase. The framework aligns to DHS guidance regarding implementation of the Acquisition Lifecycle Framework (ALF),[42] which outlines key activities for defining, developing, and delivering needed capabilities.

## A. Pre-Need

The Pre-Need phase consists of two analytical phases, a risk assessment and a capability analysis, both led by TSA's RCA. The risk assessment assesses risk to the transportation sector using intelligence, modeling, and simulation capabilities. The capability analysis includes the TSCAP that TSA began developing in 2013, and continues to integrate to create a structured, repeatable, and transparent requirements-generation process. TSCAP can be applied at three levels: holistically across TSA annually, at the program level to determine requirements for specific gaps, and on a targeted basis in response to specific needs. As of 2019, TSA's capability gaps (nonprioritized) identified in TSCAP include:

- Enhance the ability to resolve alarms;
- Enhance operators' ability to screen passengers' carry-on and checked baggage;
- Support risk-based screening wait time goals;
- Enhance the ability to verify a passenger's identification and to determine vetting status;
- Minimize physical contact with passengers;
- Reduce divestiture screening requirements;
- Enhance the ability to identify and screen a passenger and his/her baggage on the basis of an assigned risk level;
- Enhance the ability to integrate systems to support risk-based screening to support more efficient security screening;
- Secure remote access and data collection from TSE by strengthening the cybersecurity infrastructure of TSE;
- Enhance the ability to adjust security posture on the basis of risk;
- Identify traveler/nontraveling individual;
- Determine a traveler's/nontraveling individual's risk level;
- Obtain a traveler's/nontraveling individual's identified risk level;
- Dynamically adjust on-person screening parameters on the basis of a traveler's/nontraveling individual's risk level;
- Screen a traveler's/nontraveling individual's accessible property for explosives;
- Screen a traveler's/nontraveling individual's person for chemical, biological, radiological, and nuclear threats;
- Identify an aviation worker;
- Verify an aviation worker's identity;

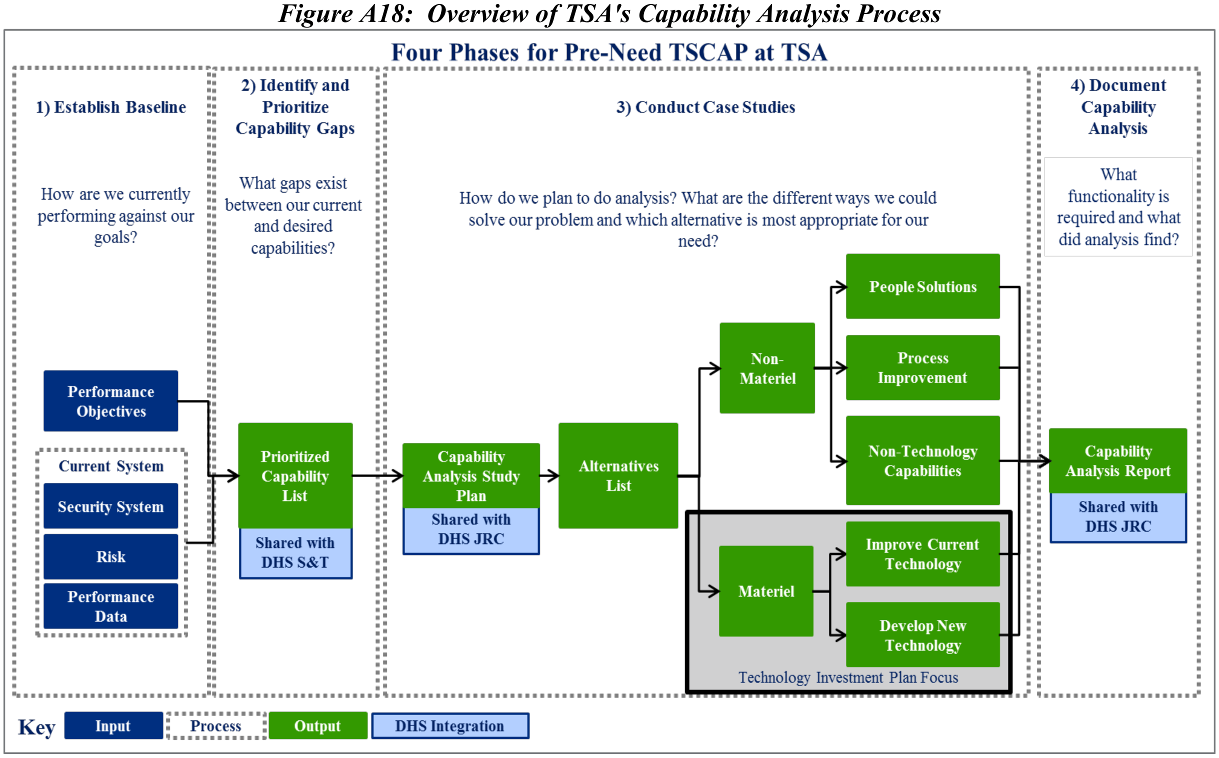
[42] DHS Acquisition Management Instruction 102-01-001, rev. 01 (March 9, 2016) and DHS Manual for the Operation of the Joint Requirements Integration and Management System, rev. 00 (April 21, 2016).

- Screen an aviation worker's person for explosives; and
- Screen an aviation worker's accessible property for explosives.

TSCAP is adapting to align to the DHS Directive 107-01,[43] which provides the overall policy and structure for the Joint Requirements Integration and Management System (JRIMS), set up and governed by the Joint Requirements Council. DHS uses the JRIMS process to review and validate capability requirements, associated gaps, and proposed mitigation options. This process helps to ensure traceability between strategic and capability investments and encourages capability development at the joint or department level.

Figure A18 shows the modified TSCAP process. The process includes collaboration with DHS by sharing the prioritized capability list during the Identify and Prioritize Capability Gaps phase; by sharing the Capability Analysis Study Plan during the Conduct Case Studies phase; and by sharing the Capability Analysis Report during the Document Capability Analysis phase.

***Figure A18: Overview of TSA's Capability Analysis Process***




TSCAP functions as an iterative process with inputs from numerous stakeholders to prioritize capability gaps across three main factors: risk mitigation trade space, strategic alignment, and network effects. This prioritization follows a structured decision-making process and results in a prioritized capability gap list used to focus TSA resources on closing critical gaps. Because of the sensitivity of the prioritized capability gap list, a deprioritized list of the most recent annual capability gap results is provided in this document. The TSCAP process includes analyzing the capability gaps to identify recommended courses of action that can help to focus TSA resources

[43] DHS Manual for the Operation of the Joint Requirements Integration and Management System, rev. 00 (April 21, 2016).

further on closing critical gaps to an acceptable level. If the only acceptable course of action is to implement a matériel solution (a new device or significant modifications to existing devices), TSA enters the ALF.

## B. Acquisition Lifecycle

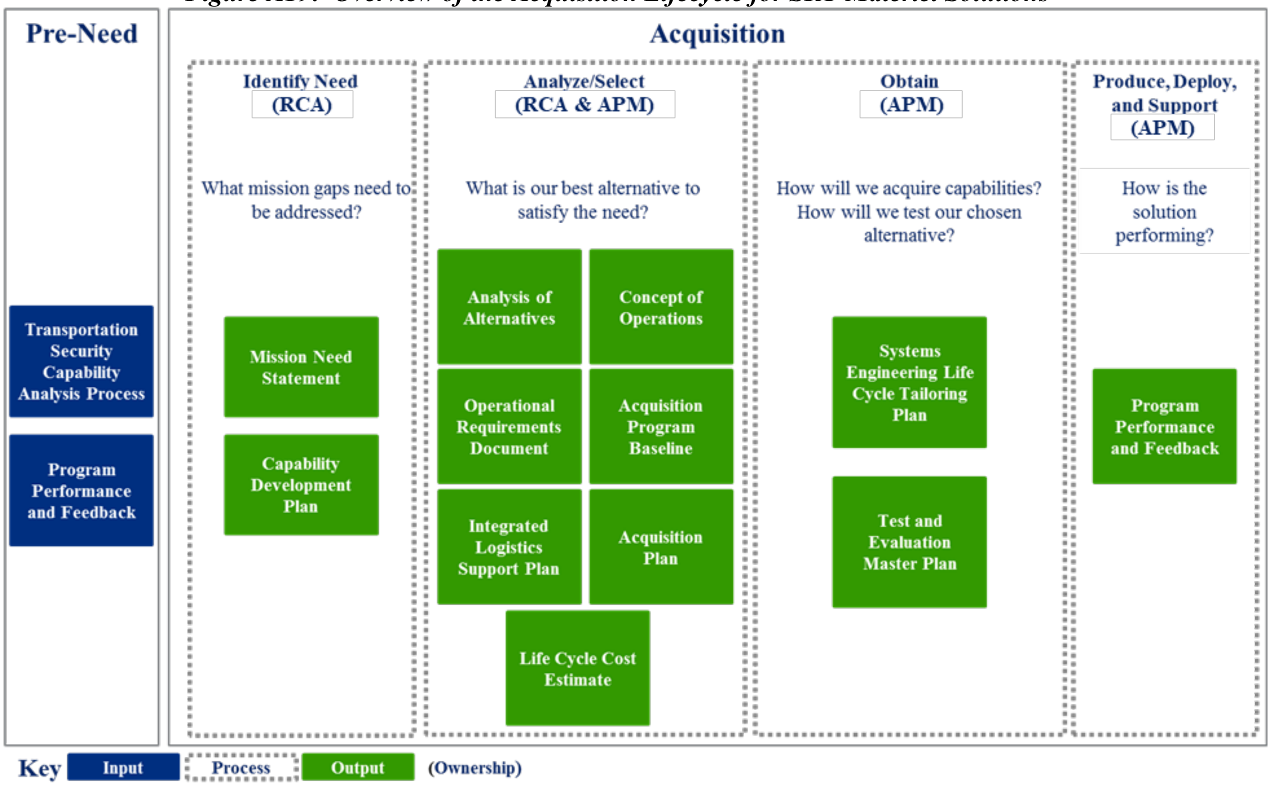
**Aligning Resources**

The first step, which is a prerequisite for an acquisition, is an analysis of resources to ensure that TSA has the correct skill sets available to support the execution of a potential acquisition or to determine how to close any gaps, if necessary. In addition to the steps addressed in the 2015 Plan, TSA also conducts annual acquisition workforce assessments in compliance with DHS acquisition program management staffing instructions to maintain consistent visibility into its workforce needs. Part of this analysis includes a comparison of TSA's staff against DHS's interpretation of U.S. Government Accountability Office guidance on acquisition program staffing. TSA further evaluates positions to determine the necessary certification levels for different job series and grades, and develops a plan during the assessment to close any gaps through hiring processes or training to ensure that it has a workforce with staff trained at the necessary levels. The Component Acquisition Executive is responsible for this step of the acquisition lifecycle.

**Identifying Needs**

TSA transitions from the Pre-Need into the Identifying Needs process of the Acquisition Lifecycle phase if the Pre-Need course of action recommended a matériel solution such as SRT, and if TSA determined that it had adequate resources to address the gap. As the lead business authority, RCA is responsible for using the capability analysis reports drafted during the Pre-need phase to develop the mission needs statement and the capability development plan with input from applicable programs. Figure A19 depicts the phases of the DHS Acquisition Management Directive 102 (AD-102) Lifecycle that have formal outputs.

*Figure A19: Overview of the Acquisition Lifecycle for SRT Materiel Solutions*[44]




## Analyzing and Selecting Alternatives

The process for analyzing and selecting alternatives remains the same as outlined in the 2015 Plan. RCA and the Acquisition and Program Management office are collectively responsible for the documents in this phase and collaborate to fulfill these responsibilities.

## 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

TSA has made strides over the past few years to maintain and further the initiatives discussed in the 2015 Plan and Strategic 5-Year Technology Investment Plan Biennial Refresh (2017 Refresh) to accelerate capability delivery and to reduce cost.[45] Below, TSA has provided updates for initiatives with significant status changes:

---

[44] The graphic does not include TSA's processes for "Aligning Resources" and "Leveraging Department Efficiencies" because they do not have formal outputs.
[45] This references page 15 of the 2015 Plan and page 9 of the 2017 Refresh.

**Transparency**

*T&E Process Guide*: The T&E Process Guide document clarifies policies and responsibilities outlined in AD-102 and DHS Management Directive 26-06.[46] TSA is updating the guide to provide more robust information to industry. The new version of the guide, which is meant to be an external document with a planned release in Calendar Year 2020, will assist industry by:

- Developing a better understanding of the T&E process,
- Detailing all phases of the T&E process, from initial planning and developmental testing to evaluation criteria,
- Identifying roles and responsibilities for key stakeholders throughout each phase, and
- Describing criteria that TSE must meet to qualify for the qualified products list.

*Transportation Security Laboratory (TSL) Deputy Director*: In 2019, the TSA Assistant Administrator of Acquisitions and Program Management (APM) and the S&T Principal Director of the Office of Innovation and Collaboration approved a memorandum of agreement to create a full-time position in TSA for a TSL Deputy Director. The TSL Deputy Director's role, among other duties, is to oversee the execution of high-level TSL strategy to support TSA mission priorities and to manage related processes in coordination with the TSL Director. This further improves visibility into TSL activities, workload, and project/initiative funding, which affects the overall execution of T&E activities.

**Accelerating Capability Delivery and Reducing Cost**

*TSA Systems Acquisitions Manual (TSAM)*: The TSAM outlines TSA's acquisition process, tailored from existing DHS acquisition policy to meet the specific needs of TSA. In accordance with AD-102, the TSAM outlines the high-level, structured approach to define, develop, and deploy capabilities in the new TSA ALF. TSAM components combine to outline a repeatable, transparent, and flexible process that acquisition teams will use when pursuing a new acquisition.

As the leadership of a TSA ALF Integrated Product/Project Team begins the process of structuring the prospective acquisition, the TSAM will guide 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, this manual enables TSA leadership to make approval decisions on the basis of a robust understanding of key decision points, processes, and stakeholders. As a keystone manual for TSA acquisitions, it will provide the foundational information that acquisition teams need to deliver the right capability at the right time.

**Deploying and Supporting SRT Technology**

TSA continues to deploy and support SRT as previously described in the 2015 Plan.[47] TSA APM is responsible for physical technology deployment.

[46] DHS Acquisition Management Instruction 102-01-001, rev. 01 (March 9, 2016); DHS Management Directive 26-06 provides DHS guidance on policies and procedures for T&E.
[47] This references page 16-17 of the 2015 Plan.

# V. Abbreviations List

| Abbreviation | Definition |
|---|---|
| AD | Acquisition Management Directive |
| ADE | Acquisition Decision Event |
| AIT | Advanced Imaging Technology |
| ALF | Acquisition Lifecycle Framework |
| APM | Acquisitions and Program Management |
| ASL | Automated Screening Lane |
| AT | Advanced Technology X-ray |
| ATSA | Aviation and Transportation Security Act |
| BLS | Bottled Liquid Scanner |
| BPS | Boarding Pass Scanner |
| C-UAS | Counter-Unmanned Aircraft System |
| CAD | Chemical Analysis Device |
| CAT | Credential Authentication Technology |
| CBP | U.S. Customs and Border Protection |
| CIP | Capital Investment Plan |
| CONOPS | Concept of Operations |
| CPSS | Checkpoint Property Screening System |
| CT | Computed Tomography |
| CTD | Checkpoint Technologies Division |
| DHS | Department of Homeland Security |
| EBSP | Electronic Baggage Screening Program |
| EDS | Explosive Detection System |
| EMD | Enhanced Metal Detector |
| ETD | Explosive Trace Detector |
| FAA | Federal Aviation Administration |
| FISMA | Federal Information Security Management Act |
| FLEx | Future Lane Experience Screening |
| FOC | Full Operational Capability |
| FY | Fiscal Year |
| FYHSP | Future Years Homeland Security Plan |
| GAO | U.S. Government Accountability Office |
| ID | Identification Document |
| IT | Information Technology |
| ITF | Innovation Task Force |
| ITIP | Information Technology Infrastructure Program |
| JRIMS | Joint Requirements Integration and Management System |
| LCCE | Lifecycle Cost Estimate |
| NEDCTP | National Explosive Detection Canine Team Program |
| O&M | Operations and Maintenance |
| O&S | Operations and Sustainment |

| Abbreviation | Definition |
|---|---|
| PC&I | Procurement, Construction, and Improvement |
| PPBE-S | Planning, Programming, Budgeting, Execution, and Strategy |
| PSC | Passenger Screening Canine |
| PSP | Passenger Screening Program |
| R&D | Research and Development |
| RCA | Requirements and Capabilities Analysis |
| RTSPA | Risk and Trade Space Portfolio Analysis |
| S&T | Science and Technology Directorate |
| SRT | Security-Related Technology |
| SST | Surface Security Technology |
| STIP | Security Technology Integration Program |
| T&E | Test and Evaluation |
| TDC | Travel Document Checker |
| TSA | Transportation Security Administration |
| TSAM | TSA Systems Acquisition Manual |
| TSCAP | Transportation Security Capability Analysis Process |
| TSE | Transportation Security Equipment |
| TSL | Transportation Security Laboratory |
| TSO | Transportation Security Officer |
| UAS | Unmanned Aircraft Systems |

# VI. Compliance Matrix

TSA's intent for the 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 3 of the Transportation Security Acquisition Reform Act (P.L. 113–245) and the Advanced Integrated Passenger Screening Technologies report as required by Senate Report 115–283 accompanying the FY 2019 DHS Appropriations Act. Figure A20 shows where in the CIP the requirements are discussed.

***Figure A20: Compliance Matrix***

| Requirement | Requirement Description | Report Location |
|---|---|---|
| b(1) | Develop 5-year technology investment plan in consultation with Under Secretary for Management. | *Not Required for Refresh* |
| b(2) | Develop 5-year technology investment plan in consultation with 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 best be addressed by security-related technology. | *System Context* – Identifying Threats |
| d(1) | The plan shall include consideration of the most recent Quadrennial Homeland Security Review (QHSR). | Most recent QHSR considered |
| d(2); d(2)A | The plan shall include a set of security-related technology acquisition needs, prioritized on the basis of risks and associated capability gaps. | *Appendix* – Transportation Security Equipment Portfolio |
| d(2)B | The set of security-related technology acquisition needs shall include planned technology programs and projects with defined objectives, goals, timelines, and measures. | *Appendix* – Transportation Security Equipment Portfolio<br>*Appendix* – Transportation Security Equipment Projects and Programs |
| d(3) | The plan shall include an analysis of current and forecasted trends in domestic and international passenger travel. | *System Context* |
| d(4) | The plan shall include an identification of currently deployed security-related technologies that are at or near the end of their lifecycles. | *Appendix* – Transportation Security Equipment Portfolio |

| Requirement | Requirement Description | Report Location |
|---|---|---|
| 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 security-related technologies expected to meet the needs under paragraph (2)-d(2)A and d(2)B | *Appendix* – Technology Investment Framework |
| d(6) | The plan shall include identification of opportunities for public-private partnerships. | *System Context* – Partnerships and Collaboration |
| d(6) | The plan shall include identification of opportunities for small and disadvantaged company participation. | *System Context* – Partnerships and Collaboration |
| d(6) | The plan shall include identification of opportunities for intragovernment collaboration. | *System Context* – Partnerships and Collaboration |
| d(6) | The plan shall include identification of opportunities for university centers of excellence. | *System Context* – Partnerships and Collaboration |
| d(6) | The plan shall include identification of opportunities for national laboratory technology transfer. | *System Context* – Partnerships and Collaboration |
| d(7) | The plan shall include 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. | *Appendix* – Technology Investment Framework |
| d(8) | The plan shall include identification of security resources, including information security resources that will be required to protect security-related technology from physical or cyber theft, diversion, sabotage, or attack. | *System Context* – Mitigating Threats |
| d(9) | The plan shall include identification of initiatives to streamline the acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation. | *Appendix* – Technology Investment Framework |
| d(10) | The plan shall include an impact assessment to commercial aviation passengers. | *Appendix* – Technology Investment Framework |
| 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. | *Appendix* – Technology Investment Framework |

| Requirement | Requirement Description | Report Location |
|---|---|---|
| d(12) | The plan shall include an identification of security-related technology interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems. | *System Context* – TSA's Future State |
| 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 sector. | *System Context* – 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. | *System Context* – Partnerships and Collaborations |
| 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. | *Appendix* – Transportation Security Equipment Projects and Programs |
| f | With the 5-yr. technology investment plan, a list of nongovernment persons that contributed to the writing of the plan shall be provided. | *Not Required for Refresh* |
| g(1) | Beginning 2 years after the date the plan is submitted to Congress under subsection (a), and biennially thereafter, the Administrator shall submit to Congress an update of the plan. | *CIP* |
| 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 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. | *System Context* – Transportation Security Equipment Acquisition Update |
| (h) | "(1) be prepared in consultation with—<br>"(B) the Surface Transportation Security Advisory Committee established under section 404; and | *Reviewed by Surface Transportation Security Advisory Committee* |
| (h) | "(2) include—<br>"(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; | *System Context* – Research and Development |
| (h) | "(B) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted; | *Appendix* – Transportation Security Equipment Acquisition Update |

| Requirement | Requirement Description | Report Location |
|---|---|---|
| (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; and | *System Context* – Transportation Security Equipment Portfolio |
| Advanced Integrated Passenger Screening Technologies | TSA is directed to submit a detailed report on passenger and baggage screening technologies not later than 180 days after the date of enactment of this act. The report shall include a useful description of existing and emerging technologies capable of detecting threats concealed on passengers and in baggage, as well as projected funding levels for each technology identified in the report for the next 5 fiscal years. | *Appendix* – Transportation Security Equipment Projects and Programs<br>*Appendix* – Transportation Security Equipment Portfolio |