U.S. Department of Homeland Security
Freedom of Information Act Branch
601 South 12th Street
Arlington, VA 20598-6020

Transportation
Security
Administration

August 31, 2020

3600.1
Case Number: 2020-TSFO-00198

Ashley Gorski
Patrick Toomey
Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
agorski@aclu.org
nspfoia@aclu.org

Dear Ms. Gorski:

This is the Transportation Security Administration's (TSA) second interim response to your Freedom of Information Act (FOIA) request dated January 09, 2020, addressed to the TSA FOIA Branch seeking access to "records pertaining to the use of facial recognition technology at airports and at the border by the Department of Homeland Security ('DHS'), U.S. Customs and Border Protection ('CBP'), and the Transportation Security Administration ('TSA')." That request seeks the following records from TSA:

1. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning:

> *a. The acquisition, processing, retention, or dissemination of data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
>
> *b. Access by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities to data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
>
> *c. Retention or dissemination by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities of data collected or generated through CBP's biometric services and infrastructure, including biometric templates.*

2. All final evaluations, tests, audits, analyses, studies, or assessments by the DHS Science and Technology Directorate, DHS Office of Biometric Identity Management, or the National Institute of Standards and Technology related to (i) the performance of algorithms in matching facial photographs, and/or (ii) the performance of facial recognition technologies developed by vendors. This request encompasses records concerning whether the algorithms or technologies perform differently based on flight route or an individual's race, ethnicity, skin pigmentation, gender, age, and/or country of origin.

3. All records, excluding informal email correspondence, concerning future interoperability between the TSA's biometric capabilities and "mission partner systems," including CBP and DHS Office of Biometric Identity Management systems.

4. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate information-sharing. [Note that we understand that in May 2020 the ACLU agreed to rephrase this request as follows: 'All policies, procedures and guidelines concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate biometric information-sharing.']

5. All records, excluding informal email correspondence, concerning the TSA's plans to "complement the capabilities" of Credential Authentication Technology through the implementation of TVS or facial recognition technology with respect to domestic travelers.

6. All records, excluding informal email correspondence, concerning whether implementation of biometric technologies would result in operational efficiencies, including whether, at certain airport facilities, "the throughput of the checkpoint may be largely unaffected" by biometric technology because "a faster [travel document checker] process would merely shift traveler volume from the queue into the screening lane."

The processing of TSA's second interim response identified certain records that will be released to you. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552. Please refer to the Applicable Exemptions list at the end of this letter that identifies the authority for withholding the exempt records by marking the block next to the applicable exemptions. An additional enclosure with this letter explains these exemptions in more detail.

For this second interim response, the TSA FOIA Branch reviewed 753 pages, of which we have released in full 211 pages, released in part (with redactions) 14 pages, withheld in full 72 pages, identified 9 pages as duplicates and 2 pages as non-responsive. Additionally, we sent 16 pages to CBP for consultation, and sent 9 pages to DHS for consultation.

We processed an additional 420 pages, which we have determined are publicly available on line at the following links:

- https://doi.org/10.6028/NIST.IR.8238
- https://www.tsa.gov/sites/default/files/foia-readingroom/final_2018_nsts_signed.pdf
- https://www.dhs.gov/sites/default/files/publications/TSA%20-%20Advanced%20Integrated%20Passenger%20and%20Baggage%20Screening%20Technologies_0.pdf
- https://www.commerce.senate.gov/2019/9/protecting-the-nation-s-transportation-systems-oversight-of-the-transportation-security-administration

The rules and regulations of the Transportation Security Administration applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 6, Part 5. They are published in the Federal Register and are available for inspection by the public.

Administrative Appeal

Because TSA's response to this request is currently the subject of litigation, the administrative appeal rights normally associated with a FOIA request response are not being provided.

If you have any questions pertaining to your request, please contact AUSA Jennifer Jude at jennifer.jude@usdoj.gov.

Sincerely,

Teri M. Miller
FOIA Officer

Summary:
Number of Pages Released in Part or in Full: 225
Number of Pages Withheld in Full: 72

APPLICABLE EXEMPTIONS
FREEDOM OF INFORMATION ACT AND/OR PRIVACY ACT

Freedom of Information Act (5 U.S.C. 552)

□ (b)(1) □ (b)(2) □ (b)(3) □ (b)(4) ☒ (b)(5) ☒ (b)(6)

□ (b)(7)(A) □ (b)(7)(B) □ (b)(7)(C) □ (b)(7)(D) □ (b)(7)(E) □ (b)(7)(F)

Enclosures

FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Transportation Security Administration (TSA) FOIA Branch applies FOIA exemptions to protect:

Exemptions

Exemption (b)(1): Records that contain information that is classified for national security purposes.

Exemption (b)(2): Records that are related solely to the internal personnel rules and practices of an agency.

Exemption (b)(3): Records specifically exempted from disclosure by Title 49 U.S.C. Section 114(r), which exempts from disclosure Sensitive Security Information (SSI) that "would be detrimental to the security of transportation" if disclosed.

Exemption (b)(4): Records that contain trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

Exemption (b)(5): Inter- or intra-agency records that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege:

- Deliberative process privilege – Under the deliberative process privilege, disclosure of these records would injure the quality of future agency decisions by discouraging the open and frank policy discussions between subordinates and superiors.
- Attorney work-product privilege – Records prepared by or at the direction of a TSA attorney.
- Attorney-client privilege – Records of communications between an attorney and his/her client relating to a matter for which the client has sought legal advice, as well as facts divulged by client to attorney and any opinions given by attorney based on these.

Exemption (b)(6): Records that contain identifying information that applies to a particular individual when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." This requires the balancing of the public's right to disclosure against the individual's right to privacy.

Exemption (b)(7)(A): Records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information…could reasonably be expected to interfere with law enforcement proceedings.

Exemption (b)(7)(C): Records containing law enforcement information when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy" based upon the traditional recognition of strong privacy interests ordinarily appropriated in law enforcement records.

Exemption (b)(7)(E): Records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Exemption (b)(7)(F): Records containing law enforcement information about a person, in that disclosure of information about him or her could reasonably be expected to endanger his or her life or physical safety.

PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

Transportation Security Administration (TSA) FOIA Branch applies Privacy Act exemptions to protect:

Exemptions

Exemption (d)(5): Information compiled in reasonable anticipation of civil action or proceeding; self-executing exemption.
Exemption (j)(2): Principal function criminal law enforcement agency records compiled during course of criminal law enforcement proceeding.
Exemption (k)(1): classified information under an Executive Order in the interest of national defense or foreign policy.
Exemption (k)(2): Non-criminal law enforcement records; criminal law enforcement records compiled by non-principal function criminal law enforcement agency; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.
Exemption (k)(5): Investigatory material used only to determine suitability, eligibility, or qualifications for federal civilian employment or access to classified information when the material comes from confidential sources.
Exemption (k)(6): Testing or examination material used to determine appointment or promotion of federal employees when disclosure would compromise the objectivity or fairness of the process.

- TSA Biometrics Informational ARB Slide Deck

The Point of Contact for this memorandum is Gary Gorrell, who may be reached at (571) 227-(b)(6) or (b)(6)

cc:
Kimberly Walton, EAA for Enterprise Support
Darby LaJoye, EAA for Security Operations
Stacey Fitzmaurice, EAA for Operations Support
Latetia Henderson, AA for Acquisition Program Management/CAE
Katrina Brisbon, AA for Contracting and Procurement/HCA
Austin Gould, AA for Requirements and Capabilities Analysis
Francine Kerner, AA for Chief Counsel
Russell Roberts, AA for Information Technology/CIO
Pat A. Rose, Jr., AA for Chief Finance Office/CFO
Kim Hutchinson, AA for Training and Development
Thomas L. Bush, AA for Intelligence and Analysis

Transportation Security Administration

TSA CLEARANCE SHEET	**ORIGINATOR**			
	Gary Gorrell			
DOCUMENT FOR ACTION	**OFFICE**	**PHONE**	**DATE**	
☒ Action Memo ☐ Letter ☐ Info. Memo ☐ Other	APM	7-(b)(6)	3/7/2019	

SUBJECT:	TSA Informational ARB ADM - Biometrics Initiative
TSA CONTROL NUMBER	APM-~~XX-XX~~ APM-19-020 *(Will be assigned when archived)*

ACTION REQUIRED

	REVIEWERS	**Office**	**Phone Extension**	**Date Received**	**Date Approved**	**Initial**	**Correction Required**
1.	CAE Staff (Jerry Schmidt/Gary Gorrell)	APM			3/7/2019		
2.							
3							
4.							
5							
6.							
7.							

****PLEASE RETURN ALL FOLDERS TO KIANA ROBINSON x7-(b)(6)***

	APM FRONT OFFICE	**INITIAL**	**DATE**	**CORRECTION REQUESTED**
1.	Lidet Makonnen/Robyn Peters			
2.	Mario Wilson			
3.	Latetia Henderson		3/7/19	

Explanation, Special Instructions, Comments:
Please return to CAE Staff once routing is complete.

[INCLUDES BIOMETRICS TEAM INPUT]

Purpose:
The purpose of this memorandum is to document the completion of the TSA Informational ARB for the Biometrics Initiative, decisions made, and action items.

Contents: ADM, ARB presentation, Sign-In Sheet.

Action Requested:
Approval and Signature

DUE DATE: 3/7/2019

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598-6028

Transportation
Security
Administration

TRANSPORTATION SECURITY ADMINISTRATION
ACQUISITION DECISION MEMORANDUM

MEMORANDUM FOR: Jason Lim
Program Manager, Biometrics Initiative
Requirements and Capabilities Analysis

FROM: Latetia Henderson 3/7/19
Component Acquisition Executive
Acquisition Program Management

SUBJECT: Transportation Security Administration (TSA) Informational
Acquisition Review Board (ARB) for the Biometrics Initiative

On March 6, 2019, the Transportation Security Administration (TSA) Component Acquisition Executive (CAE), in consort with members of the TSA Senior Leadership Team (SLT), conducted a TSA Informational Acquisition Review Board (ARB) for the biometrics initiative. The purpose of the ARB was to review the current state of the biometrics initiative and to determine the path forward.

Discussion

During the TSA Informational ARB, the biometrics team presented a comprehensive overview of: the TSA biometrics roadmap, desired TSA end state – automation of Travel Document Checker (TDC) functions via biometrics, partnership between TSA and Customs and Border Protection (CBP) concerning biometrics technology, historical biometrics pilot activities and results, current and planned biometrics pilot activities, Standard Security Program (SSP) amendment change process and how proposed biometrics-based amendments are managed from initiation to approval, TSA Modernization Act – reporting requirements and implementation, the proposed biometrics acquisition path forward using the TSA Systems Acquisition Manual (TSAM) Innovation Technology Demonstration (ITD) process, notional Fiscal Year (FY)19-20 biometrics capability development strategy, TSA biometrics architecture and design principles/target state, key policy challenges (legal, privacy, IT security), future TSA biometric capability needs at TDC and "To-Be" architecture, and the proposed agenda and speaker list for the upcoming Biometrics Industry Engagement Day scheduled to be held on March 11, 2019.

During the presentation, Mr. Gould stated that the overall goal of upcoming biometrics demonstration efforts will be to develop a validated set of requirements that can be used for future biometrics acquisition and procurement activities, as well as Public Private Partnership (P3) coordination.

FILE: 2600.3

The biometrics team stated that their near-term objective is to reach ITD Decision Point 1 by May 29, 2019.

Decisions

Based on the information presented during the ARB, the TSA CAE made the following decisions:

1. The biometrics team is authorized to implement the TSAM ITD process to further develop and define valid biometrics requirements.
2. Brian Yee has been appointed as the APM Transition Manager for biometrics.
3. Dan Thayer has been appointed as the APM Test Lead for biometrics.

Action Items

The following action items have been assigned to the biometrics team and associated personnel:

1. Internal and external stakeholder dependencies need to be identified and thoroughly defined. Project timelines and funding/investment requirements shall factor in all stakeholder dependencies.
2. Contracting and Procurement (C&P) shall be included as an active member of the biometrics Acquisition Lifecycle (ALF) Integrated Project Team (IPT) to provide input during overall strategy development efforts and subject matter expertise for follow-on activities.
3. Robyn Peters shall be included as an active member of the biometrics ALF IPT to provide P3 subject matter expertise in managing external communications and expectations.
4. The biometrics ALF IPT charter shall be finalized and published.
5. The biometrics ALF IPT shall be convened, including membership from the following offices: Information Technology (IT), APM, Requirements and Capabilities Analysis (RCA), Training and Development (T&D), C&P, Chief Counsel (CC), Policy Plans Engagement (PPE), Civil Rights & Liberties, Intelligence & Analysis (I&A), Security Operations (SO), Occupational Safety Health and Environment (OSHE), Deployment and Logistics Division (DLD), and Test and Evaluation (T&E).
6. An 1102 shall be provided by C&P and included in relevant biometrics team activities to provide subject matter expertise during the Biometrics Industry Engagement Day event.
7. Resource Allocation Plan (RAP) 21 shall include all planned biometrics activities for FY21-25.
8. A biometrics Acquisition approach tailoring memorandum from RCA to the Department of Homeland Security (DHS) Joint Requirements Council (JRC) shall be developed by the biometrics team, and approved, and sent to the JRC by the Chief Requirements Executive (CRE).
9. A biometrics approach strategy memorandum from the CAE to DHS Program Accountability and Risk Management (PARM) shall be developed by the biometrics team, and approved, and sent to PARM by the CAE.
10. The biometrics team shall meet with the Head of the Contracting Activity (HCA) to discuss procurements for upcoming biometrics demonstrations.

Attachments

TSA Biometrics

March 6, 2019

~~*WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

Transportation
Security
Administration

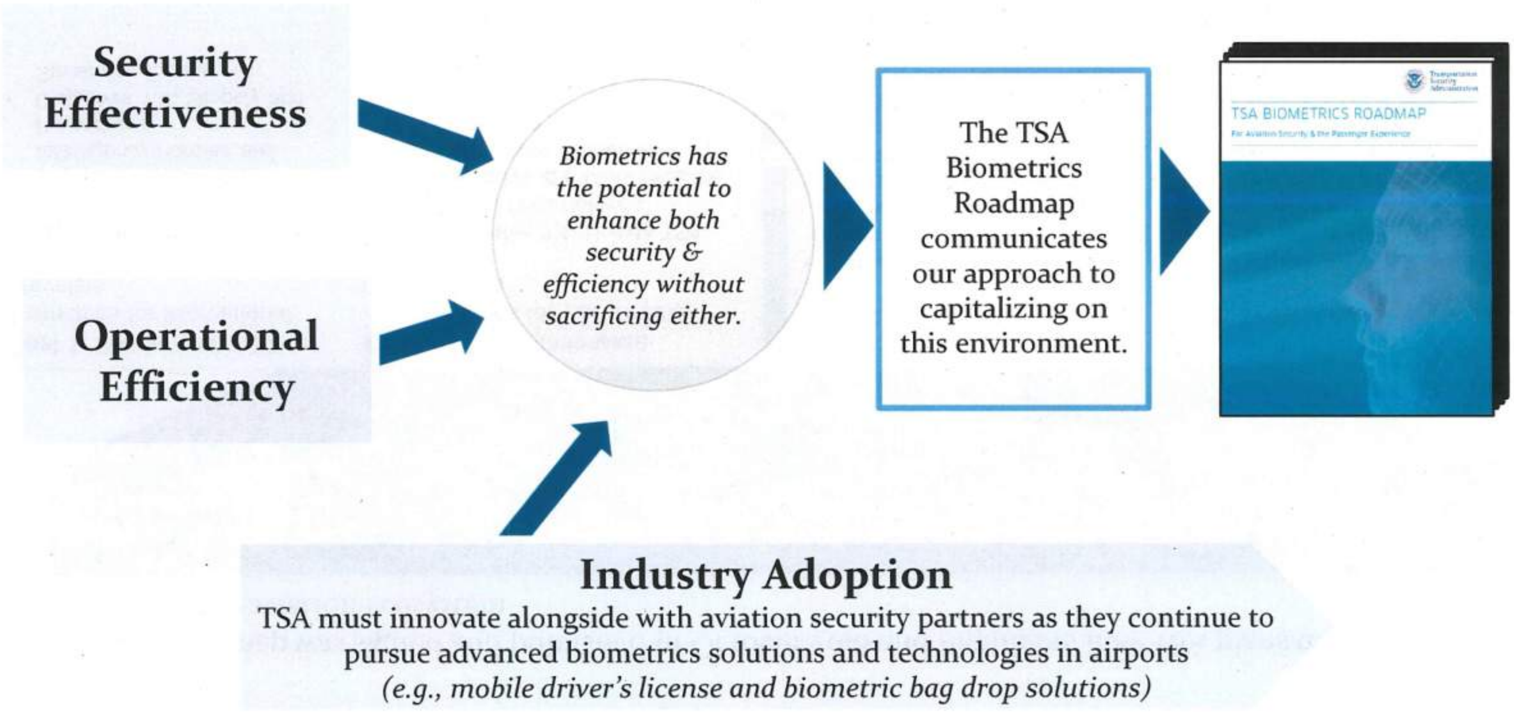
RCA | REQUIREMENTS & CAPABILITIES ANALYSIS

Biometrics Roadmap

Published Oct. 2018

Why Biometrics?

Identity verification is a cornerstone of TSA's operational landscape in the commercial aviation sector. In order to meet the challenges of evolving security threats, rising air travel volumes, resource constraints, and limits on operational footprint, TSA and aviation security regulators around the globe must look to automate manual and paper-based identity verification processes through smart technology investments.



Security Effectiveness

Operational Efficiency

Biometrics has the potential to enhance both security & efficiency without sacrificing either.

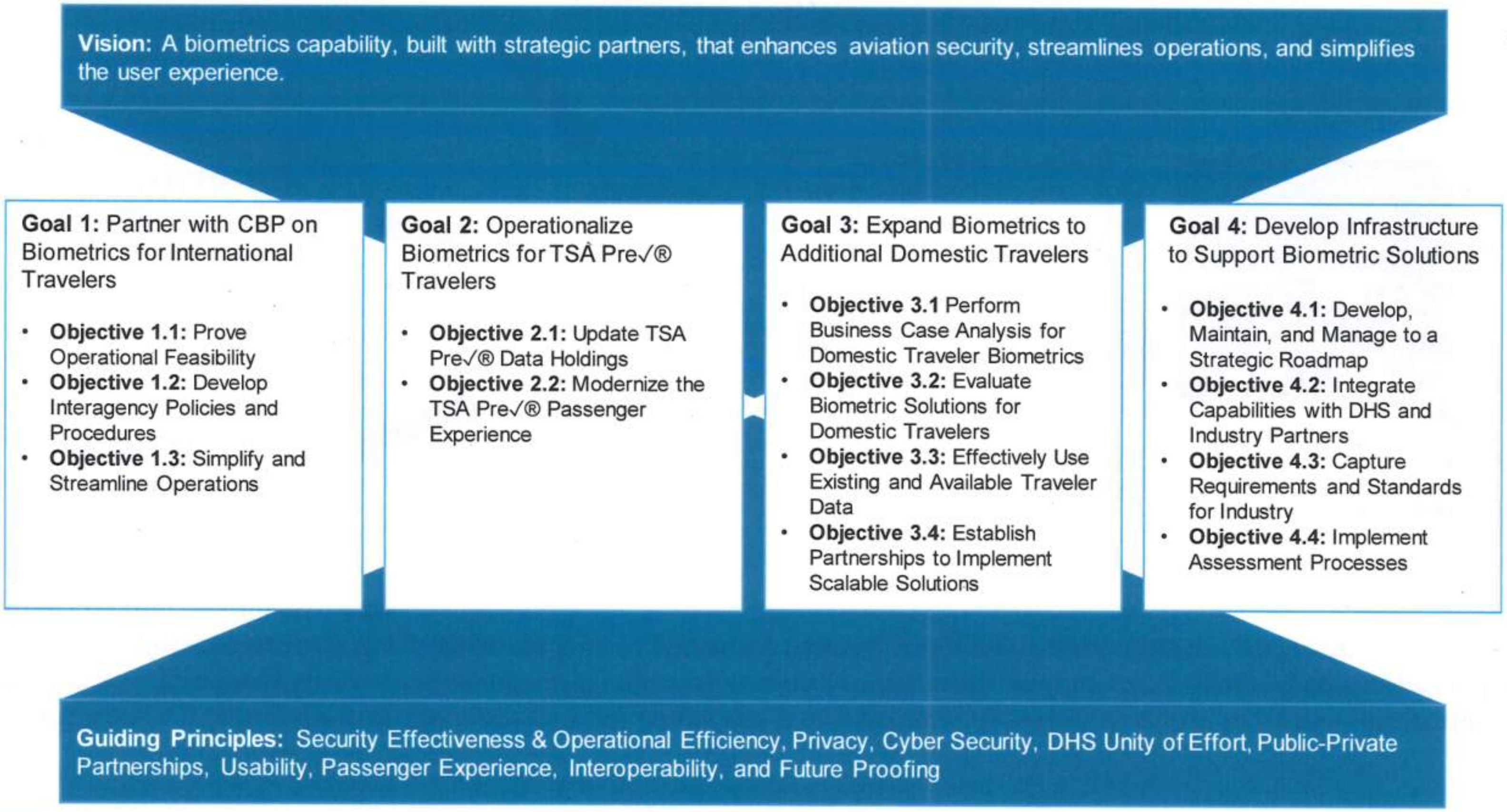
The TSA Biometrics Roadmap communicates our approach to capitalizing on this environment.

Industry Adoption

TSA must innovate alongside with aviation security partners as they continue to pursue advanced biometrics solutions and technologies in airports *(e.g., mobile driver's license and biometric bag drop solutions)*

TSA Biometrics Roadmap | Executive Summary

The TSA Biometrics Roadmap was signed and published in October 2018 and highlights how TSA plans to pursue and deploy biometric solutions for the aviation ecosystem



Vision: A biometrics capability, built with strategic partners, that enhances aviation security, streamlines operations, and simplifies the user experience.

Goal 1: Partner with CBP on Biometrics for International Travelers

- **Objective 1.1:** Prove Operational Feasibility
- **Objective 1.2:** Develop Interagency Policies and Procedures
- **Objective 1.3:** Simplify and Streamline Operations

Goal 2: Operationalize Biometrics for TSÂ Pre✓® Travelers

- **Objective 2.1:** Update TSA Pre✓® Data Holdings
- **Objective 2.2:** Modernize the TSA Pre✓® Passenger Experience

Goal 3: Expand Biometrics to Additional Domestic Travelers

- **Objective 3.1** Perform Business Case Analysis for Domestic Traveler Biometrics
- **Objective 3.2:** Evaluate Biometric Solutions for Domestic Travelers
- **Objective 3.3:** Effectively Use Existing and Available Traveler Data
- **Objective 3.4:** Establish Partnerships to Implement Scalable Solutions

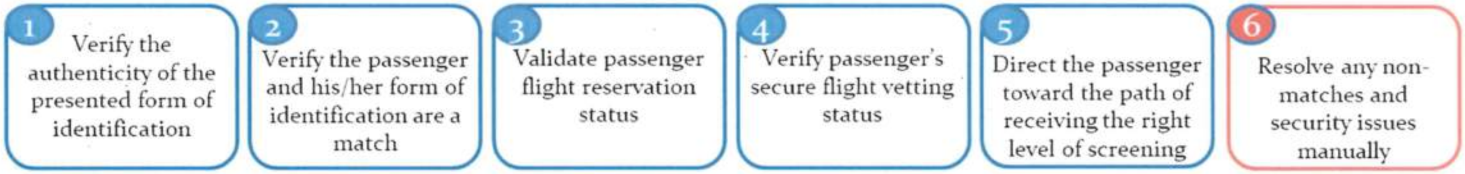
Goal 4: Develop Infrastructure to Support Biometric Solutions

- **Objective 4.1:** Develop, Maintain, and Manage to a Strategic Roadmap
- **Objective 4.2:** Integrate Capabilities with DHS and Industry Partners
- **Objective 4.3:** Capture Requirements and Standards for Industry
- **Objective 4.4:** Implement Assessment Processes

Guiding Principles: Security Effectiveness & Operational Efficiency, Privacy, Cyber Security, DHS Unity of Effort, Public-Private Partnerships, Usability, Passenger Experience, Interoperability, and Future Proofing

Desired TSA End State – Automation of Travel Document Checker (TDC) Functions via Biometrics

Prior to physical screening, TSA must:



1 Verify the authenticity of the presented form of identification

2 Verify the passenger and his/her form of identification are a match

3 Validate passenger flight reservation status

4 Verify passenger's secure flight vetting status

5 Direct the passenger toward the path of receiving the right level of screening

6 Resolve any non-matches and security issues manually

Solution Space	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Current Process (manual + boarding pass scanner (BPS))	Manual	Manual	🟨	🟨	Manual	Manual
Near Term: Credential Authentication Technology (CAT)	✓	Manual	✓	✓	Manual	Manual
Interim: Biometric ID Verification w/ SF integration	✓	✓	✓	✓	Manual	Manual
Future: Biometric ID Verification System w/ SF integration and e-Gate	✓	✓	✓	✓	✓	Manual

Key: ✓ Automated 🟨 Partially Automated

By developing an architecture that supports the automation of TDC functions, TSA can better control access to the sterile environment, improve the traveler experience, and reallocate resources to mitigate screening inefficiencies

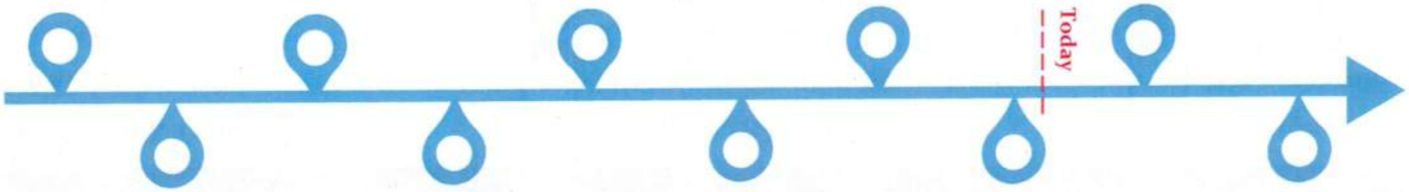
Transportation Security Administration

RCA REQUIREMENTS & CAPABILITIES ANALYSIS

CBP-TSA Partnership on Biometrics Technology

Biometrics at TSA | What Have We Accomplished?

TSA continues to refine and execute our strategy to leverage biometrics to enhance security effectiveness, increase efficiency, and improve the passenger experience



2015
Biometrics Integrated Project Team (IPT) Chartered

May 2017
Biometric Authentication Technology (BAT) contact and contactless fingerprint demonstrations at ATL and DEN

October 2017
TDC Biometrics Pilot (CBP/TSA Phase 1) at JFK Pilot matched facial photos to CBP flight galleries

January 2018
Performed Process and Technology Analysis on CLEAR

May 2018
Travel Document Checker (TDC) Process Automation Demonstration (1:1 biometric e-gate)

June-October 2018
Developed TSA Biometrics Roadmap, released October 2018

August-October 2018
TDC Biometrics Pilot (CBP/TSA Phase 2) at LAX tested the scalability of the technology with a larger gallery and enhanced automation

November 2019
ATL Terminal F pilot in coordination with CBP and Delta Airlines (curb to gate biometrics)

Late 2019/Early 2020
TDC Biometrics Pilot (CBP/TSA Phase 3) system incorporates vetting status into biometric matching

2020+
Develop and test biometric e-gate to fully automate TDC operations

Integrated Identity Verification System for Aviation Travelers

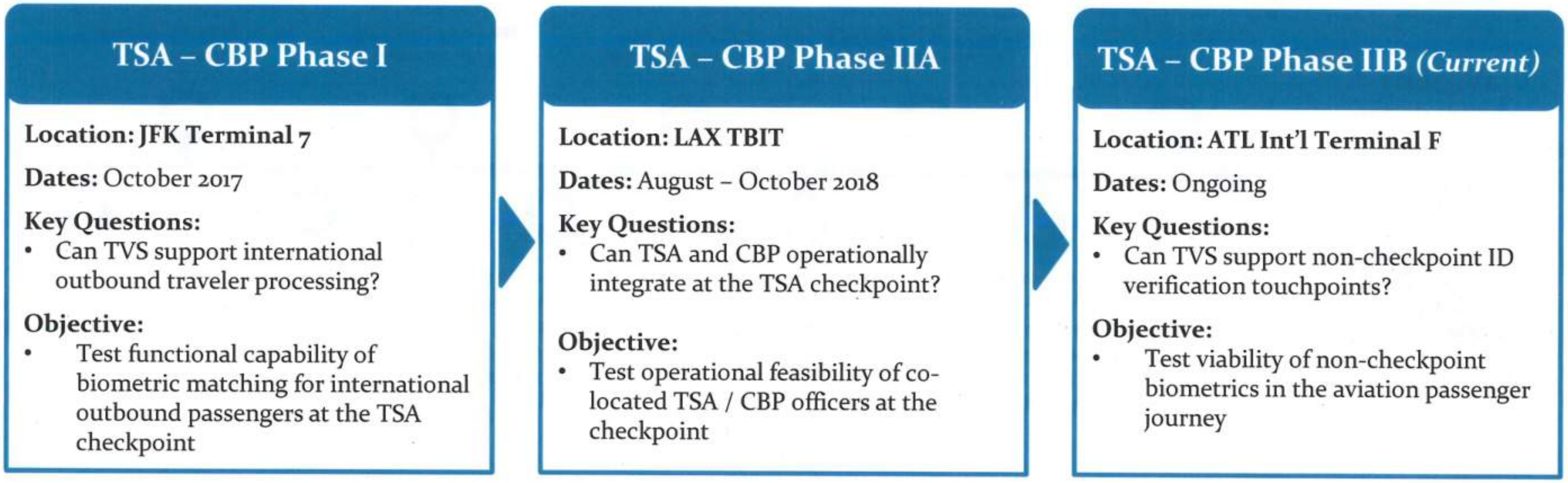
TSA is developing front-end solution requirements, designing back-end system architecture, and demonstrating innovative solutions to gain lessons learned from field operations and address capability needs.

Transportation Security Administration

RCA | REQUIREMENTS & CAPABILITIES ANALYSIS

TSA and CBP Partnership Highlights & Pilot History

Background: The "Joint TSA/CBP Policy on the Use of Biometric Technology" was signed by both organizations in April 2018. As a result, TSA and CBP have been working together on a series of phased pilots designed to demonstrate the feasibility of using biometric solutions at the TSA checkpoint. These technologies aim to automate the currently-manual TDC process, and iteratively increase operational capability over time, using a CBP-developed facial matching service called the Traveler Verification Service (TVS).



TSA – CBP Phase I

Location: JFK Terminal 7

Dates: October 2017

Key Questions:
- Can TVS support international outbound traveler processing?

Objective:
- Test functional capability of biometric matching for international outbound passengers at the TSA checkpoint

TSA – CBP Phase IIA

Location: LAX TBIT

Dates: August – October 2018

Key Questions:
- Can TSA and CBP operationally integrate at the TSA checkpoint?

Objective:
- Test operational feasibility of co-located TSA / CBP officers at the checkpoint

TSA – CBP Phase IIB *(Current)*

Location: ATL Int'l Terminal F

Dates: Ongoing

Key Questions:
- Can TVS support non-checkpoint ID verification touchpoints?

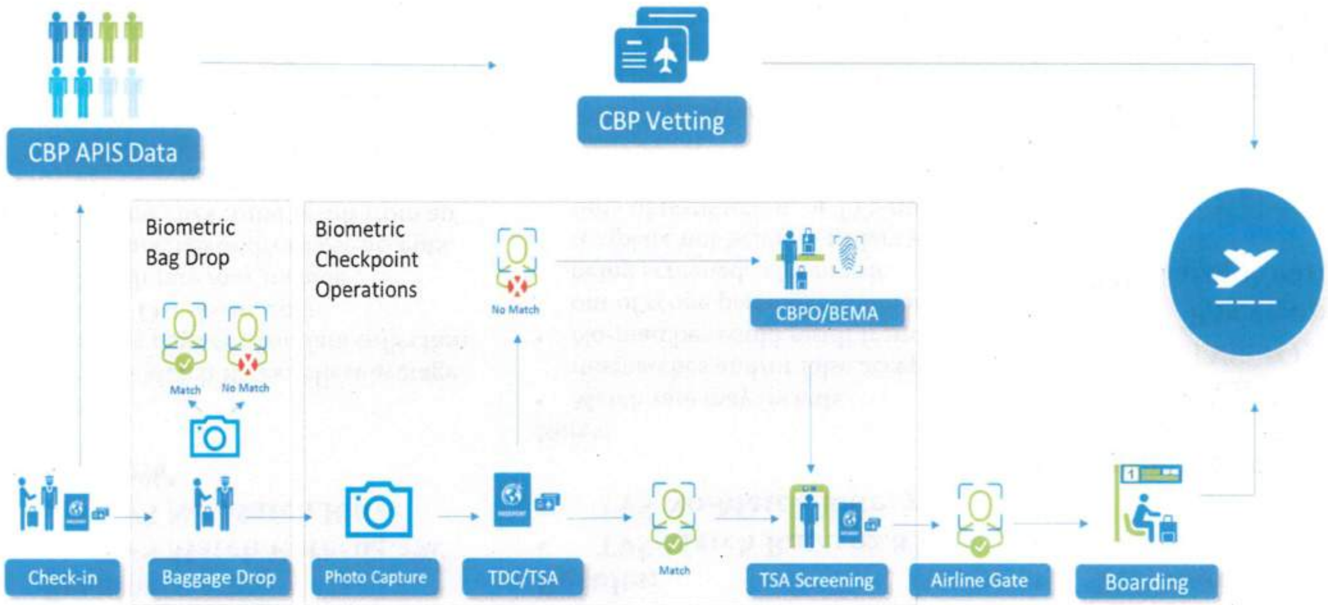
Objective:
- Test viability of non-checkpoint biometrics in the aviation passenger journey

The joint efforts by CBP and TSA have shown positive performance across various airlines, airports, and touchpoints to biometrically verify the identity of international outbound passengers.

ATL International Terminal F (Current)

The second Phase II Pilot is similar to LAX TBIT but includes additional biometric automation at TSA-regulated bag drop kiosks managed by Delta Air Lines. Sufficient test data is required for approving the AOSSP amendment for bag drop.

CONOPs OVERVIEW



CONOPs STEPS

1. Traveler checks in and proceeds to bag drop
2. Facial capture/match at bag drop eliminates the need for presentation of physical ID (license passport) for most international outbound travelers
3. Traveler is photographed prior to engaging with the TSA Travel Document Checker (TDC)
4. The matching response and limited biographic information will be displayed to the TDC on a laptop or mobile device GUI
5. TDC will scan the boarding pass to verify authenticity and the traveler will proceed to the appropriate screening lane
6. In the case where facial recognition or biographic information does not match, the TDC will process the traveler utilizing TSA's current standard operating procedures and allow the passenger to proceed to the appropriate screening lane
7. If staffing permits, CBP officers will assist with non-match resolution

Match Results from CBP-TSA Pilots

TSA – CBP Phase I

Location: JFK Terminal 7 Checkpoint

Results:

- **TVS Match Rate: 94.3%***
- **TVS No-Match Rate: 5.7%***

Notes:

- *TVS Match Rates reflect average over 5 days of pilot data collection from Oct. 16-20, 2017
- Match rate may include mismatches and/or false accepts.
- No-matches could result from an out of scope passenger (domestic) being screened, a biometric template not being in gallery at time of transaction, or TVS not being able to technically match the transaction.
- Pilot architecture/infrastructure does not facilitate documented ground truth to accurately evaluate root cause for match rates.

TSA – CBP Phase II

Location: LAX TBIT Checkpoint

Results:

- **TVS Match Rate: 92.8%**
- **TVS No-Match Rate: 7.2%**

Notes:

- Match rate may include mismatches and/or false accepts.
- No-matches could result from an out of scope passenger (domestic) being screened, a biometric template not being in gallery at time of transaction, or TVS not being able to technically match the transaction.
- Pilot architecture/infrastructure does not facilitate documented ground truth to accurately evaluate root cause for match rates.

The joint efforts by CBP and TSA have shown positive performance across various airlines, airports, and touchpoints to biometrically verify the identity of international outbound passengers.

TSA – CBP Phase II *(Current)*

Location: ATL International Terminal F

Emerging Results at Checkpoint (week of 1/26/19):

- **TVS Match Rate: 84.3%**
- **TVS No-Match Rate: 15.7%**

Emerging Results at Bag Drop (as of Dec 2018):

- **TVS Match Rate: 64.8%***
- **True Match Rate**
  - **TVS: (O: 97%, T: 90%): 99.96%**
  - **Bag Drop System: 99.87%**
- **TVS False Positive Rate: <0.1%***

Notes:

- *TVS Match Rate: Rate includes 1) in-scope passengers whose photo was not available in the gallery due to TVS sync issues, 2) processing of out-of-scope passengers, and 3) other issues with Delta DCS system.
- *TVS False Positive: TVS matched 2 in scope travelers correctly with the error coming from the NEC system sending the wrong UID to the Delta DCS due to caching. Third error occurred when an out of scope minor was processed.
- Total Number of Encounters Processed (as of 11/30): 3654
- Bag drop system accounts for all technical components DCS system, camera, TVS backend, and TVS algorithm.
- Architecture/infrastructure is in place to ground truth match results (true match and false positive) for the bag drop. Analyzing root cause of non-matches would require a means to compare ground truth from Delta's DCS to the records in the TVS gallery.

Bag Drop Amendment Process Overview

Amendment Process

- An amendment to a security program (ACISP, AOSSP, CCSSSP, CCSP-Canine, FACAOSSP, MSP, PCSSP, TFSSP) allows the aircraft operator to operate under procedures determined by TSA to provide a commensurate level of security in lieu of security program procedures.

- An aircraft operator must submit a request for an amendment to their assigned Principal Security Inspector (PSI) at least 45 days before the date it proposes for the amendment to become effective.

- TSA either approves or denies the aircraft operator's request for an amendment based on a thorough review.

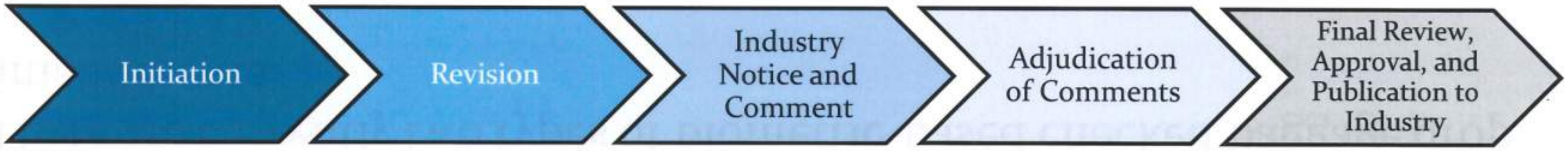
Biometric Amendments

- Policy, Plans, and Engagement (PPE) works closely with Requirements & Capabilities Analysis (RCA) to review each biometric-based amendment request separately.
    - ➢PPE will draft policy documents in conjunction with RCA's process analysis.
    - ➢Amendments based on a proof-of-concept will be reviewed and revised accordingly following RCA's test data analysis.

- There are currently two types of biometric-based checked baggage drop amendments.
    - ➢ CLEAR
    - ➢ Customs and Border Protection (CBP) Traveler Verification Service (TVS)

Security Program Change Process

Standard Security Programs (SSPs) provide specific procedures and requirements as outlined in the Code of Federal Regulations (CFR)



Initiation

- Define and agree to the scope of the SSP change
- Consult with key industry stakeholders

Revision

- Draft proposed program language with other TSA offices
- Route the proposed SSP for review and approval

Industry Notice and Comment

- Industry review of the proposed SSP change
- Submit comments to TSA
- Review of comments by TSA

Adjudication of Comments

- Draft comment responses
- Adjudicate comments with other TSA offices to finalize comment responses and program language

Final Review, Approval, and Publication to Industry

- Route the final SSP language within TSA
- Receive Administrator approval prior to publication

RCA and PPE are currently routing a memo outlining a biometrics-specific AOSSP amendment process for automating the bag drop

TSA Modernization Act Reporting Requirements

Due to Congress on July 2

TSA Modernization Act – Reporting Requirements and Implementation

On October 3, 2018, Congress passed the *TSA Modernization Act*, and it was signed into law on October 5, 2018. Section 1919 of the Act requires the Secretary of Homeland Security to submit a report to Congress, with assessments from the TSA Administrator and CBP Commissioner relating to biometric technologies, within 270 days of the law's enactment.

Summary of Section 1919

As applied **jointly to CBP and TSA**, Section 1919 ("Biometrics Expansion") of the *TSA Modernization Act of 2018* –

1. Requires the TSA Administrator and Commissioner of CBP to consult with each other on the deployment of biometric technologies
2. Requires **submission of a report** to appropriate committees of Congress (and to any member of Congress upon request) that includes assessments of:
   - The **operational and security impact** of using biometric technology to identify travelers
   - The potential **effects on privacy** of the expansion of biometric technologies, including methods proposed or implemented to mitigate privacy risks related to the active or passive collection of biometric data
   - The methods to **analyze and address matching errors related to race, gender, or age** with respect to the use of biometric technology, including facial recognition technology
3. Requires TSA and CBP to publish a public version of the joint assessment on their agency websites, if practicable
4. Requires an assessment of the biometric entry-exit system (CBP-specific)

TSA will coordinate with key agency partners, including CBP and DHS' Science & Technology (S&T) Directorate to comply with the requirements of Section 1919.

TSA Modernization Act Overarching Objectives

The following overarching objectives will guide TSA's response to the Section 1919 report

Coordinate report responses with CBP and S&T

A unified effort with key partners will be critical to ensuring the report is responsive to Congress' interest in the operational and security impact of using biometric technology to identify travelers, privacy impacts, and matching errors.

Articulate the security and operational business case for TSA's use of biometrics

Consistent with TSA's Biometrics Roadmap, the report will highlight how the use of biometrics will enhance security effectiveness, improve operational efficiency, and yield a streamlined passenger experience.

Provide transparency to Congress and the public regarding privacy protections

TSA will promote transparency to Congress and the public by engaging in careful study and analysis of potential privacy impacts. The assessment will include key privacy considerations TSA is taking into account with respect to the use of biometrics technology.

Ground efforts in rigorous academic and scientific review for a sustainable foundation

The report will provide an analysis of matching performance, which will inform both agencies' understanding of performance errors and mitigation strategies, among other findings.

Biometrics Acquisitions Path Forward

Innovative Technology Demonstration (ITD) Pathway defined in the TSA Acquisitions Manual (TSAM)

Biometrics Acquisition Path Forward

The TSA Biometrics Team proposes to use the TSA Systems Acquisition Manual (TSAM) Innovation Technology Demonstration (ITD) to find efficiencies in the acquisition process, and deliver the right technology to the field at the right time

Background

Biometrics

- TSA has been testing Biometric technologies in the field since 2015
- TSA released a Biometrics Roadmap in October of 2018, laying out intent of the Agency to explore Biometrics
- Multiple public and private partners are currently deploying or testing Biometric technologies in the aviation sector

TSAM

- The TSAM was signed in August 2018, and included the ITD process as a possible strategy to streamline acquisitions
- The ITD process allows for field demonstrations of mature technologies

ITD Process

The ITD process requires three decision points:

- **Decision Point 1: ITD Plan Brief**
    - o Approves the demonstration and initial Acquisition strategy / timeline
- **Decision Point 2: ITD Closeout Brief**
    - o Approves the demonstration results and recommends next step
- **Decision Point 3: ITD Transition Brief**
    - o Approves recommended next step and path forward

Next Steps

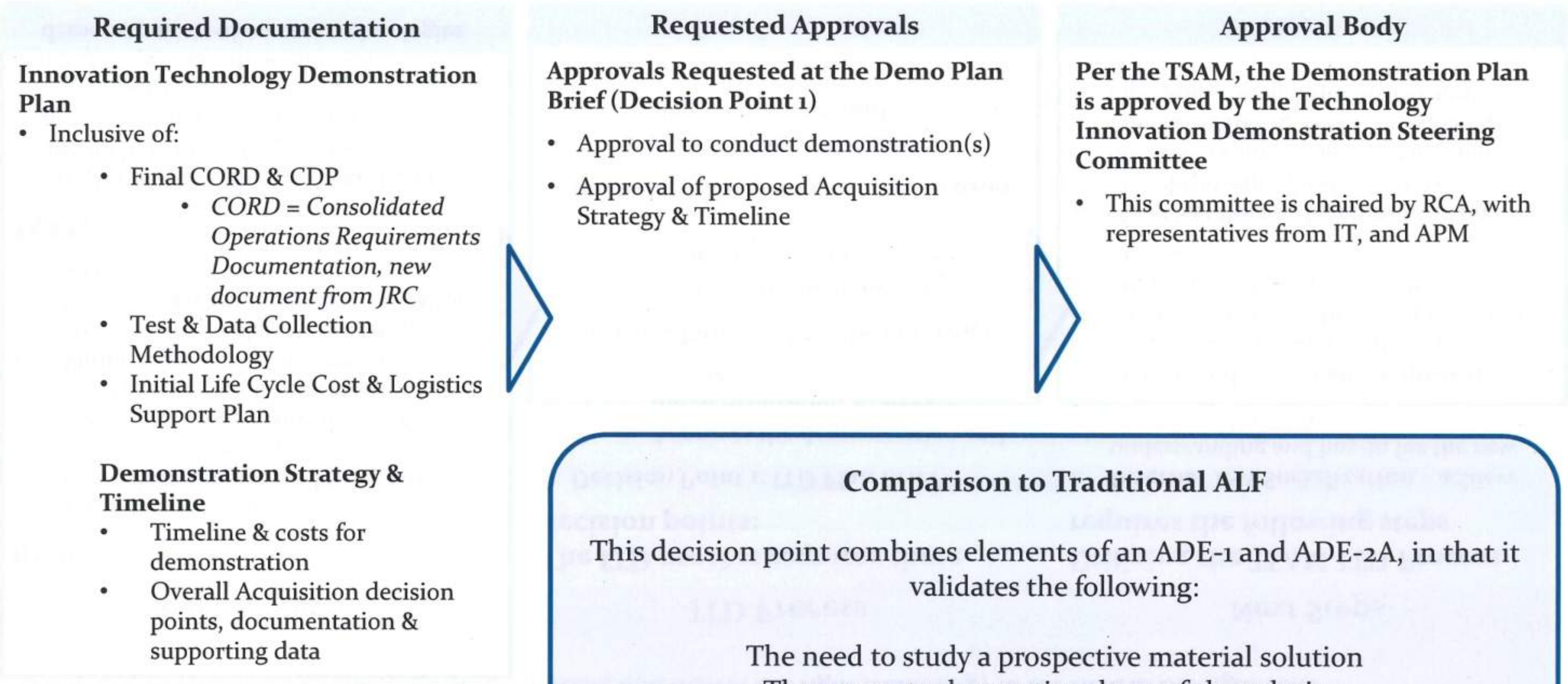
Utilizing the TSAM ITD Process requires the following steps

1. **Internal TSA Socialization** – achieve understanding and buy-in for the new process within TSA
2. **DHS Socialization and Approval** – socialize process and strategy at Departmental level to gain approval to tailor the traditional Acquisition Lifecycle
3. **Decision Point 1 Documentation Development** – begin creating documentation to support Decision Point 1, including new Consolidated Operations Requirements Document (CORD)

The TSAM ITD Process will allow for the efficient Acquisition of mature Biometrics technology, in coordination with public and private partners currently working to deploy in the aviation sector

Decision Point 1: ITD Plan Brief

The ITD process has three primary decision points, the first of which reviews the demonstration plan and path forward for the technology



Required Documentation

Innovation Technology Demonstration Plan

- Inclusive of:
  - Final CORD & CDP
    - *CORD = Consolidated Operations Requirements Documentation, new document from JRC*
  - Test & Data Collection Methodology
  - Initial Life Cycle Cost & Logistics Support Plan

Demonstration Strategy & Timeline

- Timeline & costs for demonstration
- Overall Acquisition decision points, documentation & supporting data

Requested Approvals

Approvals Requested at the Demo Plan Brief (Decision Point 1)

- Approval to conduct demonstration(s)
- Approval of proposed Acquisition Strategy & Timeline

Approval Body

Per the TSAM, the Demonstration Plan is approved by the Technology Innovation Demonstration Steering Committee

- This committee is chaired by RCA, with representatives from IT, and APM

Comparison to Traditional ALF

This decision point combines elements of an ADE-1 and ADE-2A, in that it validates the following:

The need to study a prospective material solution
The conceptual operational use of the solution
The proposed strategy to study the effectiveness of the solution

Decision Point 2: ITD Closeout Brief

The second decision point in the ITD Process validates the demonstration results and approves the appropriate transition

Required Documentation

Innovation Technology Demonstration Closeout Brief

- Inclusive of:
  - Demonstration results
  - Lifecycle Cost & Logistics Support Plan
  - Operational and Functional Requirements

Updated Acquisition Strategy & Timeline

- Proposed timeline and costs for Acquisition, procurement, and deployment
- Proposed ALF placement and decision points

Requested Approvals

Approvals Requested at the Demo Plan Closeout Brief (Decision Point 2)

- Approval of Proposed ALF Placement (or other transition)
- Approval to Propose ALF Placement to ADA

Approval Body

Per the TSAM, the Demonstration Transition is approved by the Technology Innovation Demonstration Transition Committee

- This committee is comprised of the Assistant Administrators of RCA, IT, APM, and the user office

Comparison to Traditional ALF

This decision point combines elements of an ADE-2A/B/C and ADE-3, in that it validates the following:

The need for an Acquisition program or procurement
The final operational and functional requirements
The operational effectiveness of the solution
The lifecycle sustainment plan and cost

Decision Point 3: ITD Transition Brief

The final approval in the ITD process is an Acquisition Decision Authority (ADA) approval decision, via an Acquisition Review Board (ARB), of the recommended transition

Required Documentation

Innovation Technology Demonstration Transition Brief

- Inclusive of:
  - Demonstration Closeout Brief
  - SLAs with partners and service providers
  - Deployment plan

Final Acquisition Strategy & Timeline

- Timeline and costs for Acquisition, procurement, and deployment
- Proposed ALF placement
- Proposed AD-102 documentation update timeline and plan

Requested Approvals

Approvals Requested at the Demo Plan Closeout Brief (Decision Point 2)

- Transition placement
  - According to Transition Committee recommendation, either in ALF or proceeding to Procurement

Approval Body

Per the TSAM, the final Transition decision is dependent on the approval of an TSA ARB, chaired by TSA's ADA

- Per the TSAM, the role of TSA ADA is fulfilled by the Component Acquisition Executive (CAE). Unless otherwise designated, this Deputy Administrator acts as the CAE for TSA
- ARB members include the CFO, CIO, HCA, and CC

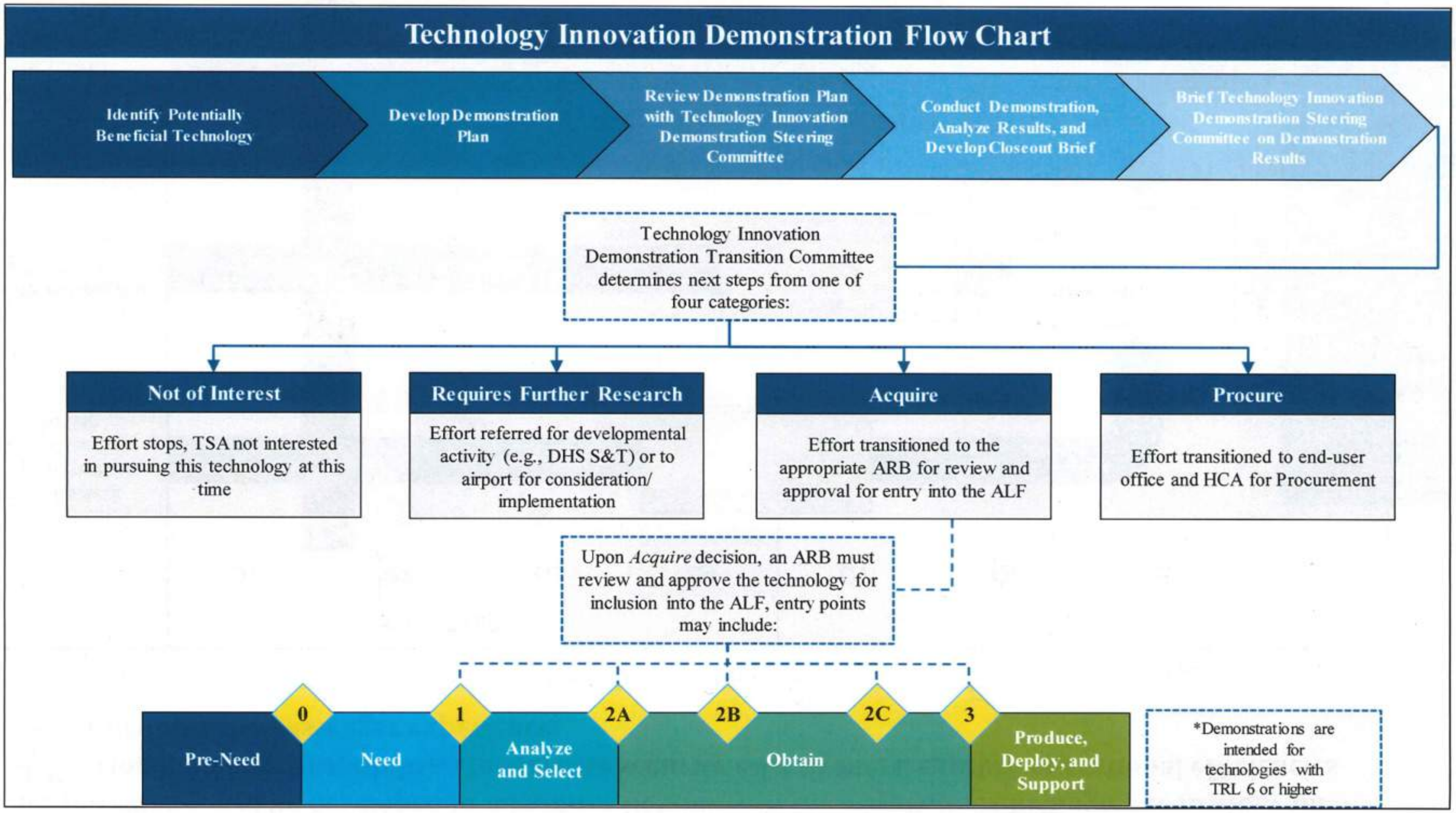
Comparison to Traditional ALF

The equivalent of this decision point in the TSA ALF is dependent on the proposed transition point. For example, if the proposed transition point is to ADE-3, this decision would mirror that ADE.

After the transition placement is approved, any ALF documentation required for compliance with AD-102 will need to be updated to official formats and routed for review as appropriate.

TSAM ITD Transition Process

The purpose of this process is to study the effectiveness of more mature technologies in the field, allowing for a potential transition into the formal Acquisition lifecycle



Technology Innovation Demonstration Flow Chart

Identify Potentially Beneficial Technology

Develop Demonstration Plan

Review Demonstration Plan with Technology Innovation Demonstration Steering Committee

Conduct Demonstration, Analyze Results, and Develop Closeout Brief

Brief Technology Innovation Demonstration Steering Committee on Demonstration Results

Technology Innovation Demonstration Transition Committee determines next steps from one of four categories:

Not of Interest

Effort stops, TSA not interested in pursuing this technology at this time

Requires Further Research

Effort referred for developmental activity (e.g., DHS S&T) or to airport for consideration/ implementation

Acquire

Effort transitioned to the appropriate ARB for review and approval for entry into the ALF

Procure

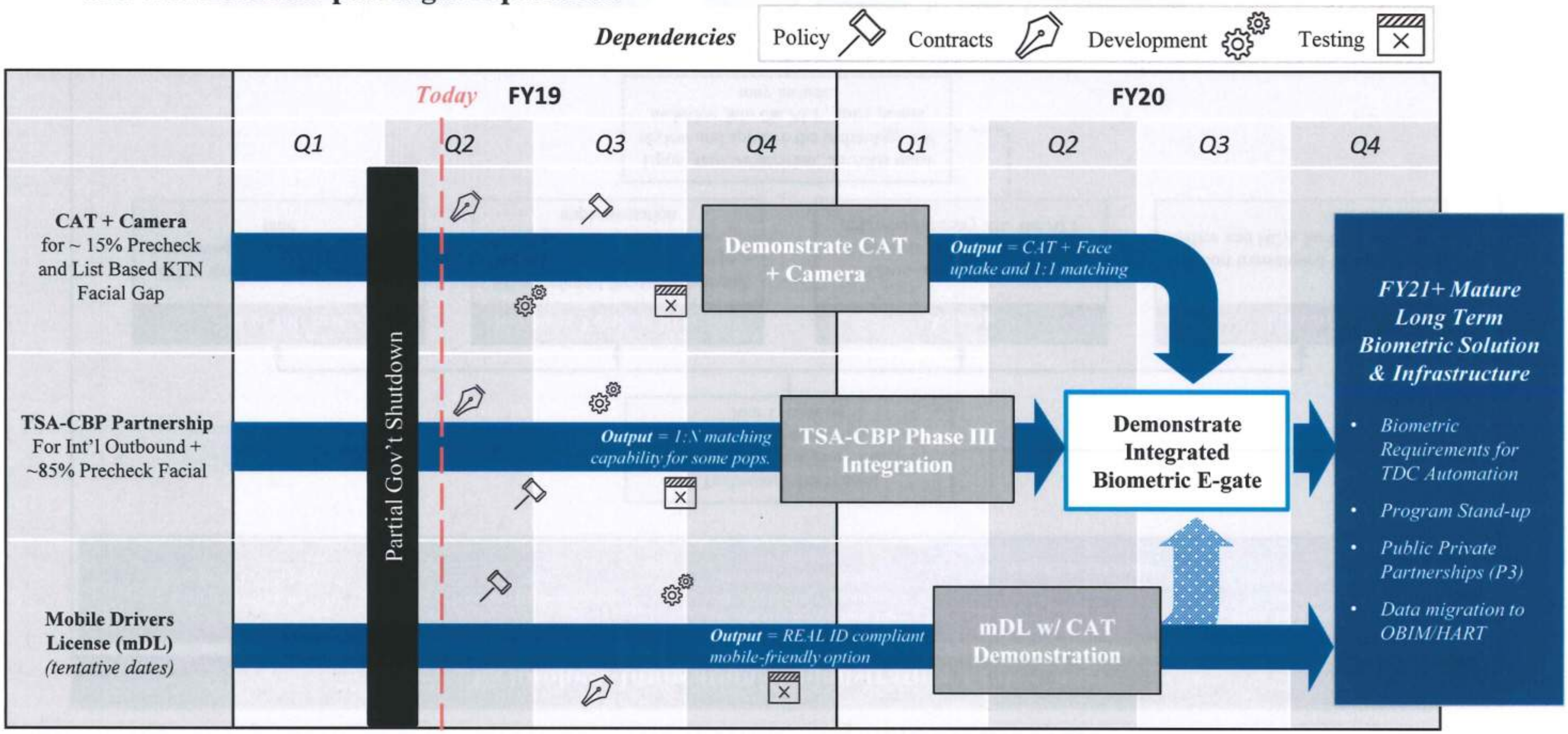
Effort transitioned to end-user office and HCA for Procurement

Upon *Acquire* decision, an ARB must review and approve the technology for inclusion into the ALF, entry points may include:

*Demonstrations are intended for technologies with TRL 6 or higher

Notional FY19-20 Biometric Capability Development

Requirements will be developed to maximize flexibility in the acquisitions/deployment strategy for delivering biometrics capabilities to increase security effectiveness, capture operational efficiencies and transform the passenger experience.



Dependencies Policy Contracts Development Testing

Today FY19 FY20

Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4

Partial Gov't Shutdown

CAT + Camera for ~ 15% Precheck and List Based KTN Facial Gap

Demonstrate CAT + Camera

Output *= CAT + Face uptake and 1:1 matching*

TSA-CBP Partnership For Int'l Outbound + ~85% Precheck Facial

Output *= 1:N matching capability for some pops.*

TSA-CBP Phase III Integration

Demonstrate Integrated Biometric E-gate

Mobile Drivers License (mDL) *(tentative dates)*

Output *= REAL ID compliant mobile-friendly option*

mDL w/ CAT Demonstration

FY21+ Mature Long Term Biometric Solution & Infrastructure

- *Biometric Requirements for TDC Automation*
- *Program Stand-up*
- *Public Private Partnerships (P3)*
- *Data migration to OBIM/HART*

Goal = Biometric E-Gate: Self service form factor integrates CAT, Biometrics, and ensures passenger is directed to correct level of physical screening

Biometric/Identity Activities

STIP Development

- Biometric Repository Upgrade
- CAT STIP Client augmented with Biometric Capabilities
- Interfaces with CBP, HART, and External entities

Prototype Unit Development

- CAT with biometrics (Two Phases)
- Biometrics Enabled TSA Technology for Identity (BETTI)- Biometric Egate
- Precheck Wayfinding Unit

Other Identity Projects

- Mobile Driver License demonstration on CAT
- McKinsey Business Case Study (OBIM funded)

Biometrics Architecture

Transportation Security Administration

RCA | REQUIREMENTS & CAPABILITIES ANALYSIS

TSA Biometrics Architecture Mission

Create an automated and scalable facial recognition capability at TDC *that enhances security, improves operational efficiency and passenger experiences, leverages enterprise investments, maximizes sustainability, and facilitates partnerships while respecting privacy, civil rights, and civil liberties*

TSA Biometrics Architecture Design Principles

TSA's Biometric Architecture design principles are grounded in the organizational mission and strategy publications below:

Key guidance supporting TSA's strategy and mission:

Maximizing what's already there

Maximize CBP and DHS investments in terms of capabilities and infrastructure in addition to what TSA has developed and validated

Privacy by Design

Assure architecture and technical solutions adhere to privacy standards and are within TSA's authorities

Simple & Consistent Experience

Create a consistent and intuitive experience for travelers and TSOs by incorporating form and human factors. Keep training and instructions simple and easy to understand for both TSOs and travelers

Open & Modular Architecture

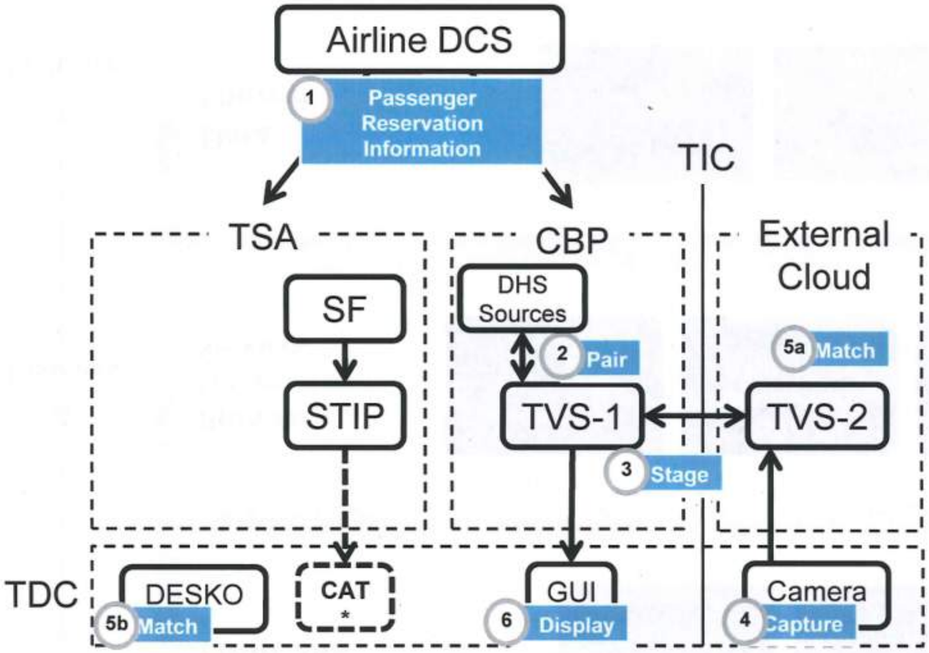
Mitigate risk of vendor 'lock-in' and allow easy Third Party integration through API-led connectivity to provide data-sharing and biometrics services

Alignment to TSA IT Vision and Security

Emphasize outcome-based security engineering considerations to maintain compliance with IT's enterprise vision and policy to create a truly secure solution

These principles were used to evaluate potential architecture paths forward and will continue to guide TSA to an optimal, future proofed biometrics capability

How it's currently being done in ATL Biometrics Pilot



Owner	Manifest	Pair	Stage	Capture	Match	Display
Airline	1					
TSA					5b	
CBP		2	3	4	5a	6

Description: *TSOs use an externally hosted, industry-owned camera to match international passengers in a commercial cloud. Match results are sent to a web-based GUI hosted on the DHS network. A DESKO is used by TSOs to scan boarding passes and manually compare with results from CBP. No capability exists to match domestic passengers without a passport.*

Flow	Description
1	Airline DCS sends flight passenger reservation information to TSA and CBP systems
2	TVS-1 pairs biographics for International Outbound passengers with photos from DHS Sources
3	TVS-1 stages flight galleries for International Outbound passengers and sends to TVS-2 for matching
4	Camera captures photo of passenger and sends to TVS-2 for matching
5a	TVS-2 matches the captured photo to the photo in the pre-staged flight gallery and shares the UID, match result, and captured photo with TVS-1
5b	DESKO confirms biographics and vetting status when passengers scan boarding pass at TDC
6	TVS-1 sends the UID, match result, captured photo, and biographics to the CBP GUI which the TSO manually verifies using the passenger's boarding pass

*Note: CAT can be used to authenticate the passenger's credentials

TSA's Evolving Environment

TSA's biometrics architecture must incorporate proven, cost-efficient technologies, leading standards, and business-centric services in order to promote long-term changeability.

Scale to TSA-specific passenger segments and meet TSA mission needs

Incorporating technological advancements to enhance security operations and mitigate bias

Adapt to regulatory and sociotechnical changes during the roll-out of new solutions

Enable Private-Public Partnership (3P) deployments through APIs and modularity

An assessment of authorities, privacy issues, costs, tradeoffs, and potential, phased courses of action will continue to inform the broader TSA biometrics solution space.

Biometrics Industry Engagement Day

Monday, March 11, 1-5pm

TSA INFORMATIONAL ARB

Biometrics Initiative

03/06/2019, 9:00 AM

Name	TSA Office	Initials
Latetia Henderson, AA, CAE	APM	
Mario Wilson, DAA	APM	MNW
Darby LaJoye, EAA	Security Operations	
Pat Rose, CFO	Chief Finance Office	
Joseph Edwards, CFO Portfolio Chair	Chief Finance Office	
Russell Roberts, CIO	IT	
Austin Gould, AA	RCA	
Keith Goll, DAA	RCA	
Thomas L. Bush, AA	I&A	
Katrina Brisbon, HCA	C&P	KBrisbon
Peter McVey, DLD DD	APM	
Andy Lee, OTA	APM	
Terry Caughran, OTA	APM	
David Cutler, Legal Counsel	CC	
Jessica Seay, Contracting Officer	C&P	
Kerry Toscano, Contracting Officer	C&P	
Holly Bolger, Contracting Officer	C&P	
Anne Cowan, User Representative	Security Operations	Present
Daniel M. Williams, User Representative	Security Operations	
Robert Harbaugh, User Representative	Security Operations	RbH
Joe Salvator, User Representative	Security Operations	
Andrea Mishoe, User Representative	Security Operations	
Mark Kenyon, Training and Development	T&D	MK
Jason Lim, PM	RCA	JL
Daniel Boyd, DPM	RCA	DB
Scott Bruner, CSID DD (Acting)	APM	
Brian Yee, CSID PPS Portfolio Manager	APM	

See Back Page

Name	TSA Office	Initials
Lidet Makonnen, Senior Advisor, Front Office	APM	
Robyn Peters, Senior Advisor, Front Office	APM	
Jerry Schmidt, AMOD DD (Acting)	APM	
Gary Gorrell, AMOD	APM	
Alex Tsurikov, AMFD	APM	
Jeremy Hodgkin, AMOD CTR	APM	
Clare O'Doherty	RCA	CSO
Justin Snyder	RCA	JMS
JOHN GATEWOOD	APM	

See Back Page

Page 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Biometric Authentication Technology (BAT) Proof of Concept (PoC) Overview

[redacted]

Transportation Security Administration

Office of Requirements and Capabilities Analysis ORCA

Agenda

- BAT PoC Overview, Objectives, and Progress
- BAT Proof of Concept (PoC) Overview
- BAT PoC Information Flow
- Checkpoint Diagram
- TSA Vision and Challenges

BAT PoC Overview, Objectives, and Progress

Below are BAT PoC overview, primary objectives, and progress to date:

PoC Overview

- Connect Known Traveler Biometrics (KTB) and Secure Flight data to the Biometric Authentication Technology (BAT) by exchanging data between Universal Enrollment System (UES) and Security Technology Integrated Program (STIP)
- Leverage TSA's existing investment in the STIP/Secure Flight interface in support of the Credential Authentication Technology (CAT)

PoC Primary Objectives

- Use TSA Pre✓® enrolled passengers in the expedited screening lane and demonstrate technical and operational feasibility of Biometric Identity Verification
- Confirm the use of BAT will not negatively impact passenger wait times and checkpoint operations

Progress To Date

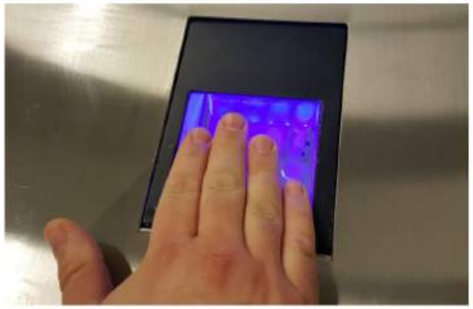
- Developed 5 contact/contactless BAT systems
- Systems are at TSIF for cybersecurity evaluation and testing
- POC tentatively scheduled to start 4/5 and ends 5/9 at DEN and ATL

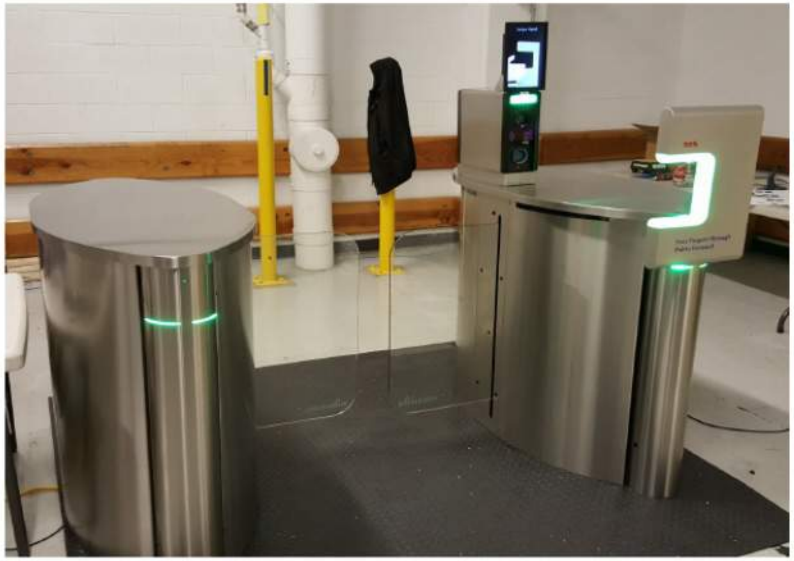
BAT Proof of Concept (PoC) Overview

Development requirements:

- Procure Commercial off-the-shelf (COTS)/ Government off-the-shelf (GOTS) fingerprint readers (3 contact and 2 contactless)
- Procure a COTS/GOTS fingerprint match algorithm
- Build a STIP BAT Client by modifying the CAT Client
- Update the STIP Enterprise system
- Assemble 5 PoC units for validation of the concept in airport environments

BAT PoC units will be fully integrated hardware and fully cybersecurity compliant, ready to connect to STIP for the PoC.



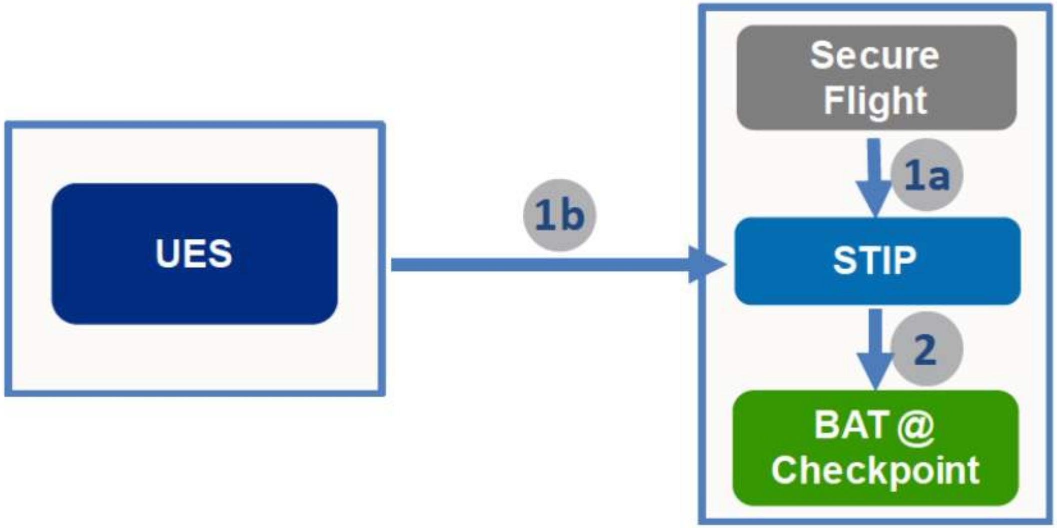


Transportation Security Administration

Office of Requirements and Capabilities Analysis ORCA

BAT PoC Information Flow

Below is the proposed information flow for the BAT PoC between Secure Flight, STIP, UES, and BAT

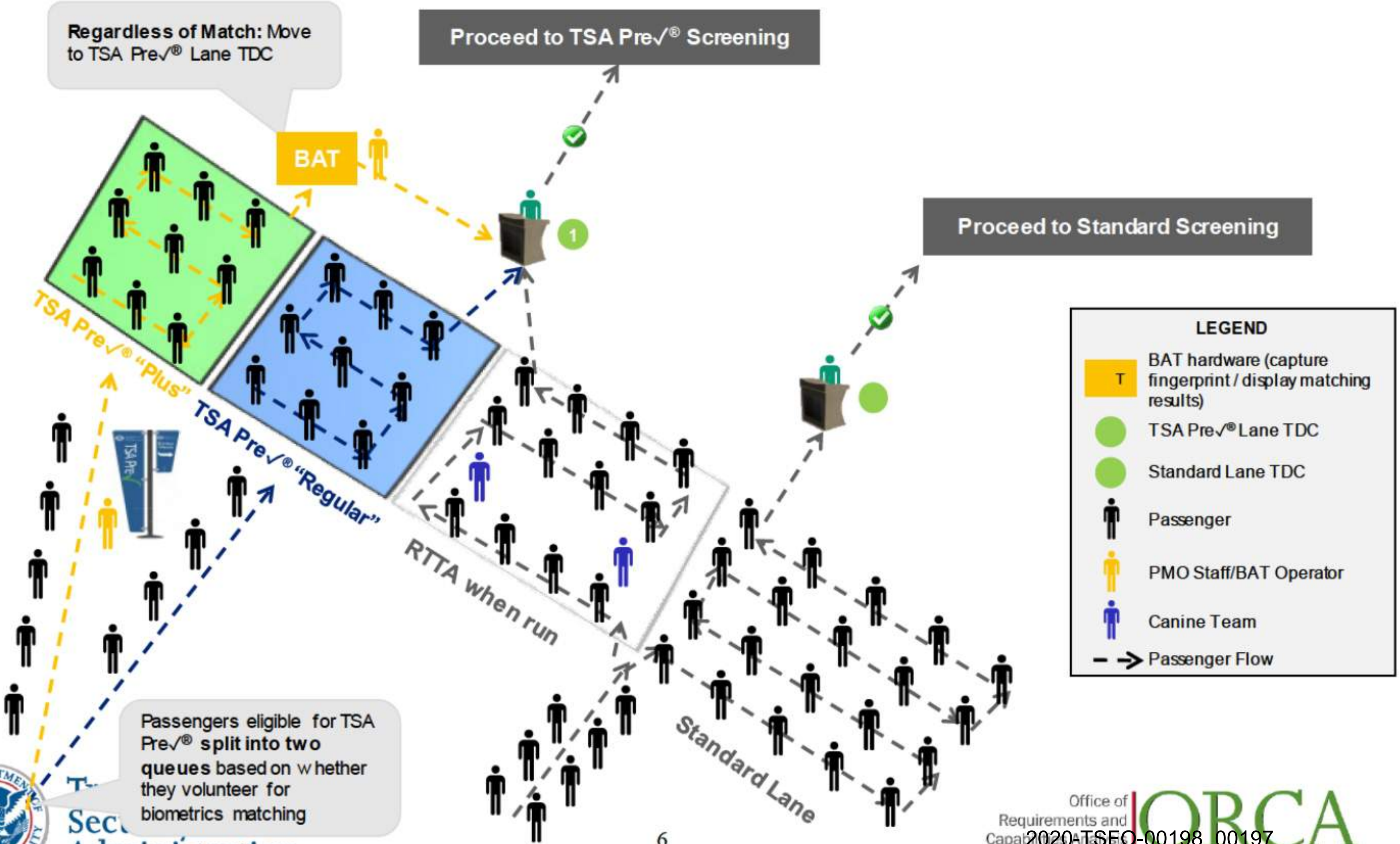


Step	Activity
1a	Secure Flight passes passenger vetting status and flight data, including TSA Pre✓® Known Traveler Number (KTN), to STIP in near real-time.
1b	UES manually sends biometrics templates and TSA Pre✓® KTN to STIP, which is put into the STIP enterprise
2	STIP passes the relevant biometrics templates retrieved from UES and passenger vetting status and flight data to the BAT device at the checkpoint

The UES to STIP information flow is completed manually (i.e., an ISSO approved method for passing data, such as an encrypted email or hand-passed thumb drive) and will not require development that does not fit into the final system architecture

Checkpoint Diagram

BAT eGate will open for all passengers regardless of biometric match. TSA Pre✓® lane TDCs will continue to verify identity for all passengers.



Regardless of Match: Move to TSA Pre✓® Lane TDC

Proceed to TSA Pre✓® Screening

Proceed to Standard Screening

Passengers eligible for TSA Pre✓® **split into two queues** based on whether they volunteer for biometrics matching

LEGEND

T BAT hardware (capture fingerprint / display matching results)

● TSA Pre✓® Lane TDC

● Standard Lane TDC

Passenger

PMO Staff/BAT Operator

Canine Team

- -> Passenger Flow

TSA Vision and Challenges

Vision

- Use biometrics at the checkpoint as the identification and boarding pass for as many passengers as possible
- Automate the Traveler Document Checker process

Capabilities

- Receive near-real time information updates from biometric repository(ies), passenger vetting service(s) (e.g. Secure Flight), and airlines
- Ensure passengers understand how to use the system
- Ensure privacy of passengers

Challenges

- Limited biometric population
- IT infrastructure development to support access to biometric repository(ies)
- Long acquisition timeline
- Policy on storage and collection
- Fully cybersecurity compliant

Transportation
Security
Administration

Office of Requirements and Capabilities Analysis ORCA

Transportation Security Administration

TSA Biometrics Capability Development

TSA is pursuing 1:1 biometric matching, 1:N biometric matching, and Mobile Drivers' License (mDL) capability integration to enhance biometrics capabilities at the TSA checkpoint for identity verification.

1:1 Biometric Matching

- **Description:** integrate biometric capture with CAT machines to verify a live image capture against a credential (e.g. a passport or ID)
- **Target Populations:** non-Trusted Travelers

~~**1:N Biometric Matching**~~

- ~~**Description:** utilize a backend repository to compare a live image capture to many enrolled references~~
- ~~**Target Populations:** Trusted Travelers, KTN holders~~

~~**mDL Capability**~~

- ~~**Description:** integrate mDL authentication capability with CAT machines to transmit digital identity information~~
- ~~**Target Populations:** All~~

TSA plans on piloting these solutions with TSA Pre✓® passengers to evaluate technology performance before deploying solutions for additional population groups

[redacted]

From: Janowski, Carol
To: Walbridge, Anne
Cc: Baker, David
Subject: RE: Biometrics Architecture Feedback
Date: Monday, May 20, 2019 12:26:50 PM
Attachments: Biometric_Placemat_2019_05_20_v1.1.pdf
TSA_Aviation_Martime_Surface_Info_Flows with BiometricOverlay_2019_05_20__V1.2.pdf
Biometrics_Landscape2019_05_20_V1.1.pdf

Anne and Dave,

Red shows were not change was made and blue shows what was updated. Please confirm you are okay with the updates.... Let me know if we should review together and I am happy to set something up at HQ in the next week or so.

I also updated the metrics based on the information provided.

Thanks for your feedback!

Biometrics Landscape

(b)(5)

Page 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: TSA OIA Correspondence
To: Operations Support; TSA OIA Correspondence; ORCA Communications
Cc: King, Chas
Subject: RE: CT-6957: [Component Action Requested] [Due 5 pm Fri 12/28] 2018 DHS Biometrics Survey
Date: Friday, February 1, 2019 12:34:26 PM
Attachments: DHS Biometrics Survey 12212018 (Attachment A) PMD Input v2.xlsx

Ops Support,

Please see the attached updated spreadsheet with an additional row (b)(5) (b)(5) This is an updated from our original submission.

Sincerely,

Chris Tobias
TSA I&A Communications
DigitalSpec LLC
(b)(6)
571-227(b)(6)

From: Operations Support
Sent: Monday, January 28, 2019 12:30 PM
To: TSA OIA Correspondence ; ORCA Communications
Cc: King, Chas ; Operations Support
Subject: FW: [Component Action Requested] [Due 5 pm Fri 12/28] 2018 DHS Biometrics Survey

Good afternoon,

Please review the attached material and complete DHS Biometrics Survey (Attachment A) **by 3pm 4Feb**.

-Please let me know if you have any questions or concerns.

V/r,

Lakiesha Smith
Program Analyst (b)(6)
Email: (b)(6)
(D): 571-227(b)(6)
(C): (b)(6)
Operations Support

From: TSA OIA Correspondence <TSA.OIA.Correspondence@tsa.dhs.gov>
Sent: Monday, December 31, 2018 2:29 PM
To: King, Chas (b)(6) Operations Support <TSA-OS@tsa.dhs.gov>; ORCA Communications <ORCACommunications@tsa.dhs.gov>
Cc: TSA OIA Correspondence <TSA.OIA.Correspondence@tsa.dhs.gov>
Subject: RE: [Component Action Requested] [Due 5 pm Fri 12/28] 2018 DHS Biometrics Survey

Good Afternoon Ops Support and RCA,

Per our Executive Director for Vetting, (b)(5) (b)(5) We're still working on our inputs and should provide before end of the week.

Sincerely,

Chris Tobias
TSA I&A Communications
DigitalSpec LLC

To: TSA OIA Correspondence <TSA.OIA.Correspondence@tsa.dhs.gov>
Cc: Walbridge, Anne (b)(6) TSA OIA PMD Comms <TSA.OIA.PMD.Comms@tsa.dhs.gov>; Ellison, Chang (b)(6)
Subject: FW: CT-6957: 2018 DHS Biometrics Survey

Good morning,

Please see PMD's input to the attached, cleared by Act DD Stephanie Hamilton. Should you have any additional questions, please contact Anne Walbridge and copy the TSA PMD Comm.

Thank you.

Marie Di Rocco
Intelligence and Analysis
Transportation Security Administration
Office: 571-227-(b)(6)
Mobile: (b)(6)
Email: (b)(6)

From: Walbridge, Anne (b)(6)
Sent: Friday, February 1, 2019 10:32 AM
To: TSA OIA PMD Comms <TSA.OIA.PMD.Comms@tsa.dhs.gov>; Hull, Jason (b)(6) Mitchell, Carolyn (b)(6)
Cc: Ellison, Chang (b)(6) Tsoi, Nathan (b)(6) Hamilton, Stephanie (b)(6) Baker, David (b)(6) Lombardo, Donald (b)(6) Boyd, Daniel A (b)(6) Janowski, Carol (b)(6)
Subject: RE: CT-6957: 2018 DHS Biometrics Survey

Good morning,

I have been coordinating with Dan Boyd in RCA and based on conversations he has had with SCO regarding this request, (b)(5) (b)(5)

(b)(5)

Jason and Stephanie, would you determine whether or not you want us to add this row? If you do, we can send this back up through Comms.

Thanks,
Anne

Anne Walbridge
Security Initiatives Lead, Program Management Division
Office of Intelligence and Analysis

From: Froemling, Hao-y Tran
To: Assili, Christine; TSA.OIA.ExecSec; Vieco, Russell E
Cc: Walbridge, Anne
Subject: RE: Joint Entry/Exit Transition Paper
Date: Tuesday, January 17, 2017 3:43:43 PM

Russ –
Should probably work with Lisa/Tom to access the actual meeting invite which has the documents that are going to be discussed/reviewed in tomorrow's meeting with CBP.

Christine –
This paper is going to be discussed at the CBP/TSA Deputies meeting tomorrow that AA Bush will be attending along with other TSA SLT.

Our main thing for the paper going up is that we are fine with the edits in the paper as we provided some of them along with other offices.

(b)(5)

Hao-y

Hao-y Froemling
Director, Program Management Division
Office of Intelligence and Analysis
TSA

Office – 571-227(b)(6)
Mobile – (b)(6)
Email – (b)(6)

From: Assili, Christine
Sent: Tuesday, January 17, 2017 12:52 PM
To: TSA.OIA.ExecSec <TSA.OIA.ExecSec@tsa.dhs.gov>; Vieco, Russell E (b)(6)
Froemling, Hao-y Tran (b)(6)
Subject: RE: Joint Entry/Exit Transition Paper

I just spoke with Rebecca

This is a paper for the DHS transition team that CBP audited. TSA provided inputs. There is no meeting specifically on this topic.
This is a recurring CBP meeting and therefore no read ahead except this paper, if the topic is

(b)(5)

Carol Melinda Janowski
Technology Solutions Division
Office of Information Technology
Department of Homeland Security
Transportation Security Administration
240-568-(b)(6) - Office
(b)(6) - Cell
(b)(6)

From: Walbridge, Anne <(b)(6)
Sent: Monday, May 6, 2019 11:02 AM
To: Janowski, Carol <(b)(6)
Cc: Baker, David <(b)(6)
Subject: RE: Biometrics Architecture Feedback

Thank you!

Anne Walbridge
Security Initiatives Lead, Program Management Division
Office of Intelligence and Analysis
Transportation Security Administration
(w): 571-227(b)(6)
(c) : (b)(6)

From: Janowski, Carol <(b)(6)>
Sent: Monday, May 6, 2019 7:04 AM
To: Walbridge, Anne <(b)(6)
Cc: Baker, David <(b)(6)>
Subject: RE: Biometrics Architecture Feedback

Anne and Dave,

Thank you for the feedback, I will make the updates this week.

Carol Melinda Janowski
Technology Solutions Division
Office of Information Technology
Department of Homeland Security
Transportation Security Administration
240-568-(b)(6) - Office
(b)(6) - Cell
(b)(6)

From: Walbridge, Anne <(b)(6)>
Sent: Friday, May 3, 2019 10:59 AM
To: Janowski, Carol <(b)(6)>
Cc: Baker, David <(b)(6)>
Subject: Biometrics Architecture Feedback

Hi Carol,

Below, please see feedback from Dave Baker and myself on the documents you provided. In addition, I've also attached the most up to date version of our population counts.

Thanks,
Anne

(b)(5)

(b)(5)

Anne Walbridge
Security Initiatives Lead, Program Management Division
Office of Intelligence and Analysis
Transportation Security Administration
(w): 571-227-(b)(6)
(c) : (b)(6)

From: Jacobs, Chandale
To: Walbridge, Anne
Cc: Jacobs, Chandale
Subject: RE: TSA - CBP LAX TBIT Biometrics IPT: Kick-off
Date: Friday, May 4, 2018 6:43:00 AM
Attachments: image001.png
TDC Baseline Proposed Metrics.docx

Hi Anne,

(b)(6); (b)(5)

Thanks,
Chandale

DHS symbol

Chandale L. Jacobs
Section Chief, TSA PreCheck Application Program
DHS/TSA/OIA/MES
Security Threat Assessment Operations
Adjudication Center
(Office): 703 487-(b)(6)
(Cell): (b)(6)
(b)(6)

From: Walbridge, Anne
Sent: Thursday, May 3, 2018 5:36 PM
To: Jacobs, Chandale (b)(6)
Subject: FW: TSA - CBP LAX TBIT Biometrics IPT: Kick-off

Hi Chandale,

(b)(5)

(b)(5)

Let me know if it would be easier to talk through this briefly – I'll have time on Friday for a quick call if that would be helpful.

Thanks again for covering all of the biometric stuff going on!
Anne

Anne Walbridge
Security Initiatives Lead, Program Management Division
Office of Intelligence and Analysis
Transportation Security Administration
(w): 571-227(b)(6)
(c) : (b)(6)

From: Manis, Rachel
Sent: Thursday, May 3, 2018 4:02 PM

To: MEDINA, CESAR (b)(6) Valdenegro, Jose (b)(6) Corgan, Kenneth (b)(6) Walton, Cornel (b)(6) Dressel, Jeffrey (b)(6) Reames, Christopher (b)(6) Schmidt, Jennifer (b)(6) GULATI, ACHAMMA (b)(6) Jacobs, Chandale (b)(6) Walbridge, Anne (b)(6) Sundquist, Lauren (b)(6) Phillips, Brandi (b)(6) Clunie, Peter (b)(6) Huynh, Tung (b)(6) (b)(6) <CTR> (b)(6) (b)(6) <CTR> (b)(6) (b)(6) <CTR> (b)(6)

Cc: Conley, Melissa (b)(6) Graviss, Matthew (b)(6) Gilkeson, James (b)(6) Hanson, Roland (b)(6) (b)(6) <CTR> (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) Kenyon, Mark (b)(6) Tsang, Elbert (b)(6) (b)(6) (b)(6) Isaacs, Bryan (b)(6) Nagy, Janis (b)(6) Cruz, Douglas (b)(6) Allicock, Nigel (b)(6) Corpuz, James (b)(6) Moreno, James (b)(6) Goldsmith, Terence (b)(6) Liston, Patrick (b)(6) (b)(6) <CTR> (b)(6) (b)(6) (US - Arlington) (b)(6)

Subject: RE: TSA - CBP LAX TBIT Biometrics IPT: Kick-off

(b)(5)

Again, we thank you for your time and will be in contact regarding next steps shortly.
Sincerely,

Rachel E. Manis
Program Manager – Detailee, Innovation Task Force
Office of Requirements and Capabilities Analysis
Transportation Security Administration

Inquiries relating to this report may be directed to me at (571) 227-(b)(6) or TSA's Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

David P Pekoske

David P. Pekoske
Administrator

2017 Annual Report On Transportation Security

Calendar Year 2016 Report to Congress

December 19, 2017

Homeland Security

Transportation Security Administration

~~**FOR OFFICIAL USE ONLY**~~

~~**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

Message from the Administrator

December 19, 2017

I am pleased to transmit the 2017 Annual Report on Transportation Security. This report combines multiple annual reporting requirements, as previously described in the Transportation Security Administration's (TSA) letter to Congress, dated August 11, 2010, in order to streamline and improve the Department of Homeland Security's processing and submission of the various annual reports on transportation security. Unless otherwise noted, the report summarizes the activities taken in calendar year 2016 by transportation systems owners and operators, and by federal, state, local, tribal, and territorial government partners to enhance systems protection and resilience for all types of hazards.

To accomplish our security mission, TSA worked collaboratively with a wide range of partners, from federal agencies, aviation and surface transportation industry stakeholders, and international counterparts to intelligence and law enforcement community professionals. We worked particularly close throughout the year with our transportation co-systems sector agencies, the Department of Transportation and the U.S. Coast Guard.

This report satisfies the reporting requirements for the following:

- Annual Periodic Progress Report on the National Strategy for Transportation Security;[1]
- Annual Report on Transportation Security;[2]
- Annual Update on Enhanced Security Measures;[3]
- Annual Report on the National Strategy for Public Transportation Security;[4] and
- Annual Report on the National Strategy for Railroad Transportation Security.[5]

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

The Honorable John Thune
Chairman, Committee on Commerce, Science, and Transportation

The Honorable Bill Nelson
Ranking Member, Committee on Commerce, Science, and Transportation

[1] 49 U.S.C. § 114(s)(4)(C).

[2] 49 U.S.C. § 44938(a).

[3] Section 109(b) of the *Aviation and Transportation Security Act* (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296.

[4] 6 U.S.C. § 1141.

[5] 6 U.S.C. § 1161

The Honorable Ron Johnson
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Claire C. McCaskill
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Michael D. Crapo
Chairman, Committee on Banking, Housing, and Urban Affairs

The Honorable Sherrod Brown
Ranking Member, Committee on Banking, Housing, and Urban Affairs

The Honorable Michael T. McCaul
Chairman, Committee on Homeland Security

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

The Honorable William Shuster
Chairman, Committee on Transportation and Infrastructure

The Honorable Peter DeFazio
Ranking Member, Committee on Transportation and Infrastructure

The Honorable Michael R. Pence
President of the Senate

The Honorable Paul Ryan
Speaker of the House

The Honorable A. Mitch McConnell, Jr.
Senate Majority Leader

The Honorable Charles E. Schumer
Senate Minority Leader

The Honorable Nancy P.D. Pelosi
House Minority Leader

Executive Summary

The 2017 Annual Report on Transportation Security fulfills multiple annual reporting requirements and summarizes activities taken in calendar year 2016 (unless otherwise noted) by transportation systems owners and operators, and by federal, state, local, tribal, and territorial government partners to enhance system protection and resilience from terrorism.[6] The report addresses modal-specific actions, as well as cross-sector and intermodal issues related to the management of risks in the Nation's transportation systems, both domestically and internationally.

The table below identifies the sector's three security goals, as stated in the 2016 National Strategy for Transportation Security, to achieve a secure and resilient transportation system. The report assesses the Transportation Systems Sector's progress toward achieving these goals and discusses key accomplishments.

Table 1: Sector Goals

Goal 1:	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Goal 2:	**Enhance effective domain awareness of transportation systems and threats**
Goal 3:	**Safeguard privacy, civil liberties, and civil rights, and the freedom of movement of people and commerce**

TSA continued to build and maintain relationships with state and local officials, owners and operators, international organizations, and U.S. Government partners to share threat information and best practices, enhance domestic and international transportation security, and coordinate the U.S. position on a multitude of security issues and mitigation measures. The Transportation Systems Sector's ability to assess security gaps, combined with practically applied risk mitigating activities, leads to continuous improvement of all activities associated with measureable threat detection, deterrence, and resilience goals, and forms the foundation of risk-based security.

[6] This report does not address activities taken in calendar year 2017, which will be covered in the 2018 Annual Report.

In 2016, TSA screened over 738 million commercial aviation passengers (more than 2 million per day and 43 million more passengers than in 2015), as well as more than 20 million airport employees. In addition, TSA officers screen 4.9 million carry-on items and 1.3 million checked items every day.[7] At domestic airports, TSA conducted random security activities, such as screening of employees, searches of vehicles approaching controlled areas, and canine sweeps. Internationally, TSA worked to influence key decision makers in foreign locations and industry partners to understand the threat, maintain awareness of vulnerabilities, and encourage operators to implement mitigation strategies.

The Maritime Transportation Subsector, led by the U.S. Coast Guard, developed tools, portals, and capabilities to more effectively share critical information. The Surface Transportation Subsector continued to identify risk and implement mitigating activities within the stakeholder and security partner areas of security operations.

The entire Transportation Systems Sector continues to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints.

[7] https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet_0.pdf

2017 Annual Report on Transportation Security

Table of Contents

I. Legislative Language

The 2017 Annual Report on Transportation Security fulfills four annual reporting requirements, including implementation of the National Strategy for Transportation Security (NSTS), and other statutory requirements, as detailed in Appendix B, to achieve efficiency and deliver a coordinated message to the President and Congress. See Appendix B for a full description of the statutory reporting requirements.

II. Sector Description, Vision, and Mission

The Transportation Systems Sector consists of a network of interdependent systems across three subsectors—aviation, surface, and maritime. The Nation's critical infrastructure depends on the transportation systems sector, and in turn, the transportation systems depend on other sectors, such as energy, communications, information technology, chemical, and manufacturing.

Interdependencies are an important dimension of the risk environment that must be considered to protect transportation critical infrastructure and achieve system resilience. A primary focus of the sector's risk management processes during this reporting period was to identify, assess, prioritize, and manage risks in order to enhance the resilience of the transportation systems.

The report describes how the transportation systems managed risk and increased resilience based on the goals and objectives stated in the 2016 NSTS. It describes progress in addressing terrorism risks, enhancing resilience, improving domain awareness, and protecting privacy, civil rights, and freedom of movement.

III. Sector Progress

This section indicates results in achieving priority outcomes. The outcomes are determined from performance data collected by government program managers or transportation operators responsible for implementing the security activities.

IV. Modal Progress

The 2016 NSTS defines goals and supporting objectives and activities for each subsector and mode of transportation. This section assesses progress toward achieving these goals by providing an overall assessment of each goal, and discussing key accomplishments in the activities that support the objectives of each goal. The transportation security community continues to enhance security through policy, programs, initiatives, and activities developed in collaboration with government and industry partners. These efforts reduce risk associated with potential terrorist attacks in part by increasing system resilience.

A. Aviation Transportation Subsector

The Aviation Transportation Subsector consists of commercial aviation, commercial airports, general aviation, and air cargo. The owners and operators, state and local authorities, and the Federal Government work collaboratively to develop measurable security activities, plans, and objectives needed to achieve threat deterrence, detection, and resilience goals.

In 2016, TSA screened more than 738 million domestic and international commercial aviation passengers. Each day, TSA screens 4.9 million carry-on items and 1.3 million checked items.[8] For the past several years, the Federal Aviation Administration/TSA Airspace Waiver Program has issued approximately 6,000 international waivers to foreign private charter and general aviation aircraft operating in U.S. airspace. The capabilities of airports to process millions of passengers and tens of thousands of tons of cargo every day depends on an estimated 1.8 million workers, most of whom undergo a security threat assessment to have access to secured areas and other Security Identification Display Areas, Sterile Areas, and/or to Air Operations Areas at U.S. airports.

Table 3: Aviation Progress Assessment

[8] https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet_0.pdf

Goal 1: Manage risks to aviation transportation systems from terrorist attacks and enhance system resilience

Overall Assessment: TSA continued to build and maintain relationships with government officials, owners and operators, civil authorities, international organizations, and U.S. Government partners to share threat information and best practices, enhance domestic and international transportation security, and coordinate the U.S. position on a multitude of security issues and mitigation measures. At domestic airports, TSA conducted random security activities, such as searches of vehicles approaching controlled areas of airports and canine sweeps. Internationally, TSA worked to influence key decision makers in foreign locations and industry partners to understand the threat, maintain awareness of vulnerabilities, and encourage operators to implement mitigation strategies. TSA continued to enhance air domain awareness with security partners and stakeholders at open-forum meetings of aviation security stakeholders.

Objective 1: Improve physical and cyber security of domestic aviation critical infrastructure

Activities:

- Increase frequency of recurrent criminal history records checks for credentialed airport workers with unescorted access to secure airport areas.
- Conduct outreach with aviation security partners on the voluntary implementation of the principles and best practices of risk management through the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[9].
- Focus security resources on high-risk travelers, workers, facilities, aircraft, cargo, and baggage.

Key Accomplishments:

- Established the Airport Operations Center, a public/private partnership, in response to the 2016 summer spike in air traffic to streamline passenger screening nationwide. Formerly called the National Incident Command Center, the Airport Operations Center provides TSA and industry with situational awareness across the Nation's busiest airports, enabling more efficient distribution of limited resources. The center tracks daily screening operations, rapidly addresses any issues that arise, and deploys personnel, canine teams, and technology where needed.

[9] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739 (February 12, 2013).

- Implemented the Federal Bureau of Investigation (FBI) Rap Back service to provide recurrent criminal history records vetting of airport workers. TSA is currently integrating all airports that elect to enroll in the Rap Back service.[10]
- Continued to work closely with industry to encourage adoption of the NIST Cybersecurity Framework and issued the Transportation Systems Sector Cybersecurity Framework Implementation Guidance document.
- Strengthened cybersecurity information sharing via the Department of Homeland Security (DHS) Critical Infrastructure Partnership Advisory Council, Aviation Government Coordinating Council, and engaged with the Sector Coordinating Council, including its Cybersecurity Working Group[11].
- Participated in the Aviation Cybersecurity Initiative, a DHS National Protection and Programs Directorate-led interagency working group that is identifying potential cybersecurity vulnerabilities in aviation and developing potential solutions to mitigate any identified vulnerabilities.
- Participated in a DHS Cybersecurity Integrated Project Team process researching "High-Priority Technology Solutions."
- Conducted the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC) pilot, an initiative to explore full-time aviation sector intelligence and information-sharing best practices across the interagency, intelligence community, and aviation private sector via a purpose-built, secure TSA facility. Government and industry assessed the pilot as high value, resulting in TSA's designation as lead of a long-term ADIAC program, endorsed by Office of the Director of National Intelligence, DHS, and Aviation Sector Coordinating Council.
- Increased the number of deployed Passenger Screening Canine teams.
- TSA issued an information circular recommending that airports and airlines perform insider threat self-vulnerability assessments. The results were analyzed and recognized practices were shared with airports and airlines for their consideration when implementing risk mitigation plans.

Objective 2: Improve preparedness and response capabilities to deter, detect, respond, and recover from terrorist attacks throughout the aviation community

[10] The FBI Rap Back Service provides airport authorities the capability to receive immediate notification of criminal and, in limited cases, civil activity of enrolled individuals that occur after the initial processing and retention of criminal or civil fingerprint transactions. The service is available to all commercial airport operators; however, for airport operators to participate in the Rap Back program, the airport operator must, among other things, sign a memorandum of understanding with TSA that documents its participation in the program. By the end of 2016 TSA had executed over 50 memoranda of understanding with airport operators and plans to enroll additional airports in 2017.

[11] The Critical Infrastructure Partnership Advisory Council provides the operational framework for the sector partnership structure and is aligned with the National Infrastructure Protection Plan and Presidential Policy Directive-21.

Activities:

- Improve training for frontline employees to identify, deter, prevent, and respond to threats to the homeland.
- Execute and enhance vetting of passengers and aviation credential holders, as well as indications and warning of potential threats to aviation sector.

Key Accomplishments:

- Centralized the training of newly hired Transportation Security Officers (TSO) at the TSA Academy at the Federal Law Enforcement Training Center. By the end of 2016, nearly 6,000 new hire TSOs were trained at the TSA Academy.
- Developed and implemented Mission Essential Threat Mitigation training to integrate intelligence threat awareness, security capabilities and operational training for TSA frontline workforce in order to sustain security effectiveness. Developed quarterly updates for employees in order to maintain this skillset.
- Conducted in-service training for all TSOs and supervisors to address security vulnerabilities identified in several Office of Inspector General Reports. The Mission Essentials Training series focused on the links between threat intelligence, checkpoint technologies, operational procedures, and the TSO's role in mitigating threats. The first iteration of this training was completed in September 2015 and is now conducted several times a year with each session focused on a different topic to enhance threat mitigation and improve screening operations.
- Institutionalized training and development across the employee career lifecycle. TSA developed the Management, Administrative, and Professional new-hire training course into a mandatory, five-day, in-residence program it piloted in fiscal year 2017. This training focuses on the history of TSA, its national security mission, and the frontline operations that employees support. Additionally, TSA began planning and developing the TSA Leadership Institute, to target current employees promoted to critical positions and positions of leadership.
- All Transportation Security Executive Service employees attended leadership training at Harvard's National Preparedness Leadership Initiative to institutionalize common leadership concepts and provide tools for leading through crisis and change.
- TSA developed a threat-based operational training course for new Federal Security Directors and Deputy Federal Security Directors. This comprehensive program, which began in 2016, includes classroom instruction, coaching, and mentoring components.
- Enhanced TSA's Insider Threat Program and outreach to stakeholders to support development of similar programs across all of the nation's commercial airports.
- Developed and provided Insider Threat Awareness training for aviation sector personnel, emphasized through training and awareness campaigns, such as "See Something, Say Something ™" and "This is My Airport."
- Instituted a new concept of operations to enhance and focus risk-based planning and deployment of Visible Intermodal Prevention and Response (VIPR) teams to mitigate potential threat actors in the aviation domain.

- Implemented automated passenger prescreening and review of lost and stolen passports submitted as part of a Secure Flight Passenger Data submission.
- Improved the identification of selectee matches by refining the Secure Flight automated matching threshold and date of birth algorithm for Expanded Selectee List matching.
- Initiated an independent assessment of the effectiveness and reliability of the Secure Flight vetting engine/algorithm responsible for watchlist matching.
- Increased the use of Secure Flight Passenger Data to strategically deploy Federal Air Marshal teams aboard U.S. flagged commercial flights to mitigate potential threats.
- The Homeland Security Advanced Research Projects Agency developed an Emerging Explosive Threats training course to familiarize operators and facilitate discussion with TSA staff on homemade explosive threats and concepts, explosive detection technology fundamentals, and capabilities.

Objective 3: Enhance international aviation security risk management strategies

Activities:

- Conduct outreach to facilitate the use of international best practices and procedures.
- Assess compliance with security measures for international inbound passengers, cargo, and baggage.

Key Accomplishments:

- Enhanced security effectiveness and mitigated risks to global aviation by providing assistance to all last point-of-departure airports through a variety of activities, such as outreach, training, technical expertise, capacity development, and on-the-spot counseling.
- TSA conducted 135 foreign airport assessments; 1,880 air carrier inspections; and 47 capacity development training activities for 31 countries.
- On September 22, 2016, the United Nations Security Council adopted Resolution 2309, focusing on the threat posed by terrorism to civil aviation. The Department of State and TSA were full partners in ensuring this document represented the collective vision of all nations to secure the world's air transportation system. It calls on all States to work within the United Nations International Civil Aviation Organization (ICAO) to ensure that its international security standards are reviewed and adapted to effectively address the terrorist threat to civil aviation. TSA is working with ICAO to develop the Global Aviation Security Plan.

Objective 4: Increase security technology capability to respond to known and emerging threats

Activities:

- Improve industry participation in the Research and Development (R&D) process for threat detection and screening capabilities.

- Improve aviation safety and security capabilities to detect illegal use of unmanned aircraft systems (e.g., integrated tracking mechanisms).

Key Accomplishments:

- The TSA Innovation Task Force collaborated with airports, airlines, and the aviation industry to foster innovation, advance aviation security, and improve capabilities in the checkpoint with a focus on preserving effectiveness while driving efficiency.
- Facilitated discussion among regulated parties that use transportation security equipment at the annual TSA Industry Day – Innovating Our Future Symposium, held June 7-9, 2016. This event resulted in a list of more than a dozen issues frequently experienced by end-users that will be presented to vendors at the next annual Air Cargo Industry Day, providing direct access to aggregated feedback from end-users to improve products and services in support of increased screening effectiveness.
- Established phase-out requirements for all Explosives Trace Detection (ETD) devices and single-view x-ray machines currently on the Air Cargo Security Technology List to increase the level of performance of industry-owned and operated equipment. This will result in the need for air cargo regulated end-users to replace these ETD devices by 2021 and single-view x-ray machines by 2020. The phase-out program ensures deployed equipment meets TSA requirements and addresses emerging threats.
- Conducted data collection and analysis in collaboration with Air Cargo ETD test bed participants to generate insights about system lifecycle performance, operational activity, and environmental considerations. This facilitates improvement of detection capability requirements and enhancement of next generation ETD devices. The ETD test bed serves as a prototype for other air cargo technology test beds.
- Continued to evaluate the suitability and effectiveness of air cargo screening at six test bed locations under the Infrastructure Protection and Surveillance Field Assessment Program.
- Qualified new devices for the Air Cargo Security Technology List, which expands the number of qualified systems and allows industry increased flexibility in decisions about which screening technologies best fit its security needs.
- Coordinated with the DHS Science and Technology Directorate (S&T) to identify risk-based capability gaps and establish engineering development programs for emergent technologies. Using these gaps, the DHS S&T Homeland Security Advanced Research Projects Agency posted Broad Agency Announcements to solicit technologies that address the capability gaps.
- Provided insider threat program training, awareness and shared best practices to enhance partner strategies in mitigating potential threats from insiders.
- Received approval for automated access to five additional Terrorist Identities Datamart Environment category codes, which makes it possible for TSA to make informed security threat assessment decisions for individuals seeking access to critical and sensitive transportation infrastructure. TSA is coordinating with relevant departments and agencies to determine the efficacy of vetting TSA's credentialed population against one additional TIDE category code.

- To complement location-specific mitigation activities, TSA provided international stakeholders with training and materials to raise awareness of insider threat risks throughout the international aviation security community. TSA presented a paper on insider threat risk awareness and mitigation at the ICAO Aviation Security Panel and General Assembly as well as various regional fora, such as the Latin American Civil Aviation Commission. TSA also delivered 18 insider risk capacity development training courses across Europe, Africa/Middle East, and the Western Hemisphere.

Goal 2: Enhance effective air domain awareness of transportation systems and threats

Overall Assessment: The Aviation Subsector continued to enhance air domain awareness with security partners and stakeholders in 2016 at open-forum meetings of aviation security stakeholders, such as those held by the Aviation Security Advisory Committee (ASAC), and the Aviation Government Coordinating Council and Sector Coordinating Council. The Aviation subsector worked with its security partners to assess the security at airports, analyze the aviation security attack scenarios posing the greatest risk, develop mitigation plans to address the highest priority areas, and share intelligence and best practices.

Objective 1: Improve quality and timeliness of intelligence and information products for government, industry and public awareness

Activities:

- Improve public awareness of security issue reporting channels and dissemination of actionable threat information among partners (e.g., “If You See Something, Say Something™”, General Aviation Watch program, and “This is My Airport”).
- Expanded information sharing with industry through classified and unclassified fora, such as monthly airport security teleconferences, and general aviation coordination during National Special Security Events and other events for which the Federal Aviation Administration issues security-related temporary flight restrictions.

Key Accomplishments:

- Produced and disseminated 43 Country Threat Assessments looking at international threats to U.S. civil aviation and Western interests. Conducted 52 unique in-person engagements consisting of threat briefings to individual airlines and trade associations and site-visits to industry facilities, providing timely and accurate information to industry partners.
- Produced the 2016 Annual Civil Aviation Threat Assessment and the 2016 Annual Transportation Cyber Threat Assessment.
- Began a pilot program for the City and Airport Threat Assessment system, with full implementation anticipated by the end of calendar year 2017.
- Developed enhancements for the Last Point of Departure Threat Model, with a pilot program anticipated to begin by the end of calendar year 2017.

- Conducted the Annual Transportation Sector Security Risk Assessment, which assessed that the overall risk to aviation increased in 2016 due primarily to increasing threats associated with Islamic State of Iraq and Syria and foreign fighters.
- Approximately 68 Field Intelligence Officers and 14 Liaison Officers provided direct support to TSA field locations and representation at partner organizations. Field Intelligence Officer staffing increased by 17 to expand coverage and intelligence support. Field Intelligence Officers also delivered more than 5,103 intelligence briefings as part of TSA's overall Mission Essential Threat Mitigation training program to increase security effectiveness of the TSA frontline workforce, and delivered 496 intelligence briefings to aviation stakeholders.
- Completed the ADIAC pilot, an Office of the Director of National Intelligence (ODNI)-sponsored test bed for a single aviation domain sharing hub for the dissemination of intelligence and threat-related information to a growing network of industry and agency partners.
- Streamlined the process for sharing TSA suspicious incident reporting with local, state, tribal and territorial, and federal criminal justice agencies through the FBI's National Data Exchange system.

Objective 2: Improve collaboration among private sector and government agencies regarding intelligence and information sharing

Activity: Increase discussion of strategic priorities as an agenda item at open-forum meetings of aviation security stakeholders. Examples include Public Area Security Summit and ASAC meetings.

Key Accomplishments:

- Participated in the Quarterly Airport Security Review with the airport industry, which has led to meaningful collaborative sessions to update current security policy and provide strong joint efforts on new initiatives.
- Continued to implement recommendations provided by the ASAC on aviation workers' access to security restricted areas.
- Participated on several working groups with stakeholders on issues including policy and planning, cargo, risk-based security, and contingency planning.
- Conducted the 2016 ADIAC pilot, an initiative to integrate full-time aviation sector intelligence and information-sharing best practices across the interagency, intelligence community, and aviation private sector at a secure facility.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: The Aviation Subsector continues to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints. The DHS

Traveler Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs. The Aviation subsector also improved the efficiencies of security measures for passengers by increasing enrollment in expedited screening programs, such as TSA Pre✓® application program and other DHS trusted traveler programs. TSA public outreach efforts ensured a smoother travel experience for passengers, especially as the agency introduces new security protocols amid a constantly evolving threat environment.

Objective 1: Reduce the potential negative impact of security policies and activities to privacy, civil rights and civil liberties

Activity: Develop policy pursuant to applicable privacy, civil liberties, and civil rights laws and regulations.

Key Accomplishments:

- Performed significant outreach and training to field operations to address transgender passenger complaints regarding screening.
- Expanded the customer service program AskTSA to additional social media applications, which is designed to improve the passenger experience and to better assist them before, during, and after their flight.
- Processed 1,698 redress requests with an average response time of 44 days, which improves on the DHS High Priority Performance Goal of less than 60 days.

Objective 2: Apply risk-based security approach to supply chain and traveler movements

Activity: Enhance efficiency and effectiveness of cargo and traveler screening.

Key Accomplishments:

- Increased TSA Pre✓® application program enrollment by 113 percent to 4.2 million enrollees, allowing these prescreened low-risk travelers to experience expedited, more efficient security screening and enhancing the overall efficiency and effectiveness of the screening process.
- More than 26.5 percent of all passengers were screened via TSA Pre✓® lanes in FY16.

B. Maritime Transportation Subsector

The U.S. maritime transportation system is a vital part of the national economy, playing a key role in the global supply chain. It consists of 25,000 miles of navigable channels, 238 locks at 192 locations, and over 3,700 marine terminals at 360 ports. Waterborne cargo and associated activities contribute more than $649 billion annually to the U.S. Gross Domestic Product and sustain more than 13 million American jobs.[12] More than 99 percent of the volume of overseas trade enters or leaves the United States by ship.[13] By their nature, the seas and oceans are generally less restricted and are freely accessible to transit without many of the mechanisms for detection and investigation often available in the air and land domains. Maritime security vulnerabilities and the potential consequences from a variety of hazards, including hurricanes, terrorist attacks, and cyber threats continue to be significant.

The U.S. Coast Guard (USCG) and its partners maintain a suite of performance measures to monitor progress in meeting Maritime Transportation Security Act (MTSA) performance goals and objectives. Refer to the following reports for further information on key maritime security related performance and metrics:

- Maritime Administration Annual Report to Congress, 2013;
- DHS Annual Performance Report for Fiscal Years 2016-2018;
- U.S. Customs and Border Protection (CBP) 2016 Annual Report;
- Threat of Terrorism to U.S. Ports and Vessels Report to Congress, dated September 26, 2014; and
- Department of Homeland Security 2016 Annual Performance Report (for the DHS Domestic Nuclear Detection Office and Science and Technology Directorate).

Table 4: Maritime Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience
<u>Overall Assessment</u>: The Maritime Transportation Subsector continues to work with security partners and stakeholders to pursue a risk-based security posture. With the signing of the National Strategy for the Waterside Security of Extremely Hazardous Cargos (September 1, 2015), the Hazardous Cargo Transportation Security Subcommittee was re-established within the Chemical Transportation Advisory Committee to work along with the National Maritime

[12] Maritime Administration, *Marine Transportation System Important Facts*. Available at http://www.marad.dot.gov/ports_landing_page/marine_transportation_system/MTS.htm. Accessed May 23, 2016.

[13] Ibid.

Security Advisory Council to assist the USCG in developing policies and procedures to deny the use of hazardous cargos as weapons.

Objective 1: Utilize risk-based security planning and operations to reduce the terrorism risk to the MTS
Objective 2: Reduce security vulnerabilities and improve preparedness throughout the MTS

Activities:

- Expand cybersecurity protections in all segments of the MTS using the NIST Framework.
- Improve compliance at MTSA facilities through risk-based adjustment of enforcement operations tempo.
- Improve interoperability of federal, state, local, tribal, and territorial response teams in Maritime Security and Response Operations.
- Employ a Maritime Security Risk Analysis Model and other risk assessment and analysis tools to refine the estimates of maritime security and response operations activities' risk reduction benefits and use these estimates to inform the execution of Maritime Security and Response Operations activities in U.S. ports.
- Improve International Ship and Port Facility Security Code implementation in foreign ports that send ships to the United States.
- Explore potential use of floating security barriers at critical infrastructure and key resources to provide deterrence and resilience.
- Conduct random, unpredictable operations, such as Visible Intermodal Prevention and Response (VIPR) team deployments, to mitigate terrorist risk to the traveling public and maritime infrastructure.

Key Accomplishments:

- The USCG's International Port Security Program conducted assessments of 150 foreign ports in 50 countries in 2016 while imposing conditions of entry on vessels arriving from 17 countries. The International Port Security Program also conducted 40 capacity building activities in 18 countries with marginal port security, in order to prevent them from falling into non-compliance with the International Ship and Port Facility Code.
- The USCG screened more than 117,000 Notices of Arrival and Departure, 32.4 million crew/passenger records, and released 54 spot reports for national security, terrorist, law enforcement, or regulatory concerns.
- Vessels that visit countries, ports, and facilities not maintaining effective anti-terrorism measures as determined by the USCG's International Port Security Program are examined to verify that enhanced security measures were implemented while the vessel visited a non-compliant country/port/facility. In 2016, the USCG conducted 1,657 Condition of Entry verification exams.

- Enrolled approximately 505,000 workers in the Transportation Worker Identification Credential (TWIC®) program[14], for a program total of 3.6 million, providing a security threat assessment and tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities and vessels regulated under the MTSA, and all USCG credentialed merchant mariners.
- The USCG enforced TWIC® regulations in the maritime domain. In 2016, 53,978 TWIC® verification checks were conducted through a combination of visual inspection and the use of biometric card readers.
- USCG facility inspectors and facility security officers conducted 5,912 MTSA facility inspections that aim to prevent maritime transportation security incidents and marine casualties resulting from malicious acts, accidents, or acts of nature against waterfront facilities.
- Instituted a new concept of operations to enhance and focus risk-based planning and deployment of VIPR teams in an unpredictable and random manner in the maritime domain.

Goal 2: Enhance effective domain awareness of maritime transportation systems and threats

Overall Assessment: The Maritime Transportation Subsector developed tools, portals, and capabilities to more effectively share critical information. The USCG continues to work with security partners on enhancing Maritime Domain Awareness tools and capabilities. Specific focus has been to improve the reporting of cyber-related security incidents and modification to the MTS Recovery Common Assessment and Reporting Tool to include new categories of Essential Elements of Information this year.

Objective 1: Improve the security, resilience, and regulatory (federal/state/local/tribal/territorial) information sharing process throughout the MTS community
Objective 2: Improve MTS stakeholder participation in the risk management process for security and resilience prioritization and programming

Activities:

- Enhance Maritime Domain Awareness tools and capabilities.
- Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of data from the Maritime Security Risk Analysis Model.
- Enhance resilience of cyber systems through expanded exercises and assessments.

[14] Required by the MTSA (Pub.L. 107–295) for workers who need unescorted access to secure areas of the nation's maritime facilities and vessels.

Key Accomplishments:

- Working with the Department of Transportation (DOT) and TSA, the USCG developed Enhanced Coordination Procedures in accordance with directives outlined in Presidential Policy Directive-41 (PPD-41), titled "United States Cyber Incident Coordination." PPD-41, published on July 26, 2016, defines what constitutes a cyber incident and more importantly, who is responsible for responding to a significant cyber incident. Enhanced Coordination Procedures are designed to enhance unity of effort and ensure that consistent response procedures are developed, deployed, and updated as appropriate.
- Developing Homeport 2.0[15] to provide a better user experience and improve the security of user information. Planned upgrades include fewer site navigation menus, and more efficient and secure search functions.
- Worked with the National Maritime Security Advisory Council, the National Offshore Safety Advisory Council, and many individual industry associations to share cyber information, and to understand the best mechanisms for sharing cyber-related security information.
- The USCG continues to manage, monitor, and update the MTS Recovery Common Assessment and Reporting Tool program to support field personnel with port recovery and status reporting.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

Overall Assessment: The Maritime Subsector continues to work with its security partners and stakeholders on privacy and the civil rights and liberties of individuals and entities to ensure the freedom of movement. The USCG revised key policies and practices with regard to this goal.

Objective: Collaborate with international partners to increase the resilience of key foreign ports and foreign infrastructure critical to the MTS and global supply chain

Activities:

- Enhance joint CBP/USCG practices and use of the Maritime Infrastructure Recovery Program for the expeditious recovery of trade after an attack.
- Enhance preparedness of ports through the Area Maritime Security Committee Improvement Process.

Key Accomplishments:

- Issued the revised CBP/USCG joint protocols.

[15] The USCG Homeport Internet Portal, established in 2005, facilitates compliance with the requirements set forth in MTSA, by providing secure information dissemination, advanced collaboration, electronic submission and approval for vessel and facility security plans, and complex electronic and telecommunication notification capabilities.

- Using the Area Maritime Security Training and Exercise Plan, federal Maritime Security Coordinators and their Area Maritime Security Committees tested the effectiveness of their respective port-level Area Maritime Security Plans and supported maritime security preparedness regimes through the engagement of federal, state, local, tribal, and territorial government and private sector stakeholders. In 2016, a total of 93 events were held, including 11 seminars, 4 workshops, 28 table top exercises, 11 functional exercises, 21 full-scale exercises, 12 area maritime security drills, 1 area maritime security game, and 5 maritime security operations during real events receiving exercise credit. Each event generated remedial actions for improving maritime security and identified best practices that were shared with the Area Maritime Security Committees.

C. Surface Transportation Subsector

The Surface Transportation Subsector enhances security through a risk-based approach to prevent terrorist attacks, protect people and critical assets and systems, and support response to national transportation security incidents. The subsector consists of four transportation modes: Mass Transit and Passenger Rail, Freight Rail, Highway and Motor Carrier, and Pipeline.

The strategy is to identify risk and implement mitigating activities within the stakeholder and security partner areas of security operations. The subsector's ability to analyze gaps identified by a vulnerability assessment process and apply practical mitigating activities leads to continuous improvement of activities associated with the threat detection, deterrence, and resilience goals.

Changes to policy, regulations, legislation, or budget are identified in this annual review where necessary. These assessments highlight issues associated with the NSTS implementation strategies, information sharing and risk analyses that continue to advance progress of NSTS goals, objectives, and activities.

Table 5: Mass Transit and Passenger Rail (MTPR) Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience
Overall Assessment: Security partners and stakeholders in the MTPR mode continue to pursue a risk-based security posture. TSA, security agencies, and the operators jointly pursued policies to secure surface systems, including implementing exercises and training, physical

~~**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

and cyber hardening measures and operational risk deterrence activities. Two examples include the Amtrak-led Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE), [16] and the VIPR Program. These activities provide heightened station and right-of-way patrols, increased security presence onboard trains, explosives detection canine sweeps, random passenger bag inspections, and counter-surveillance.

Exercises and training programs assisted industry operators in directing resources and efforts towards effectively reducing risks. TSA facilitates Intermodal Security Training and Exercise Program (I-STEP) exercises helping transportation entities test and evaluate their security plans, including prevention and preparedness capabilities, response abilities and cooperation with first responders. In addition, the Exercise Information System (EXIS), which is a TSA-sponsored online exercise tool, guides government and industry users through the exercise planning process and provides resources to design, document, and evaluate exercises for all transportation modes.

Objective 1: Sustain effective security assessments and planning in the critical mass transit and passenger rail industries through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences

Activity: Develop, periodically review, and update security plans based on available information.

Key Accomplishments:

- Baseline Assessment for Security Enhancement (BASE) reviews were completed at all high-risk MTPR agencies due for reassessment. BASE includes an evaluation of the agency's established written security programs and emergency management plans. Each agency received a rating of 100 percent in this category, meaning that all high-risk MTPR agencies had satisfactory security programs and plans.
- TSA continued its collaboration with industry to assess infrastructure vulnerabilities. The TSA MTPR test bed program has provided marketplace and emergent technologies assessments, and improvements in security for over twelve years, averaging at least ten surface transportation test beds per year. Examples include insertions of second and third generation standoff at range Person-Borne Improvised Explosive Device detection technologies, pilot testing and recommendations for evolution of under-vehicle screening at speed technologies, and significant breakthroughs in advanced infrastructure protection. Several of these technologies have be used at National Special Security Events. TSA also maintains a chemical/biological detection technology testbed in a high risk transportation facility in the Northeast.

[16] Operation RAILSAFE, a partnership by the Amtrak Police Department, New York City Police Department, and TSA deploys law enforcement officers from local, state, federal, rail and transit agencies at passenger rail and transit stations and along the right-of-way to exercise counterterrorism and incident response capabilities.

- In partnership with the DOT Transportation Technology Center, TSA continued to assess the vulnerabilities of mass transit and passenger rail vehicles through modeling and simulation and live explosive validation.
- Instituted a new Concept of Operations to enhance and focus risk-based planning and deployment of VIPR teams in an unpredictable and random manner in the MTPR domain.

Objective 2: Provide effective security training for frontline employees of mass transit and passenger rail entities

Activity: Conduct training of frontline employees to enable them to identify, prevent, deter, and respond to threats.

Key Accomplishments:

- The BASE reviews conducted at high-risk agencies, i.e., those with at least 60,000 daily unlinked passenger trips, measured their progress in establishing and mainting a Security and Emergency Training Program. Results indicated that 78% of those systems assessed received a passing score equal to or greater than 70 percent.
-
- Delivered approximately 31,850 Counterterrorism Guides to 8 transit organizations, the American Public Transportation Association, and 15 TSA Surface Inspector field offices. Also provided over 12,500 Cyber Counterterrorism Guides to 13 MTPR organizations and 8 TSA Surface Inspector field offices for expanded distribution to appropriate frontline employees as part of a cooperative effort to improve MTPR system security.
- Published the Security Training for Surface Transportation Employees Notice of Proposed Rulemaking and the Surface Transportation Vulnerability Assessments and Security Plans, Advance Notice of Proposed Rulemaking with consideration given to Goal 3 intent and objectives during draft/review processes.

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Mass transit and passenger rail systems either conduct or participate in exercises designed to evaluate the preparedness for, and response to, security events.

Key Accomplishments:

- Through the I-STEP, TSA completed six exercises, in line with program targets and goals: Dallas, Texas; San Antonio, Texas; Philadelphia, Pennsylvania; Washington, DC; and Denver, Colorado (two). Additionally, TSA rolled out the EXIS in-person to MTPR systems in six cities: Oklahoma City, Oklahoma; Portland, Oregon; Houston, Texas; Stockton, California; Charlotte, North Carolina; and Columbus, Ohio. Best practices and lessons learned were derived and developed as a result of these exercises and distributed to industry.

- VIPR Personnel supported nine iterations of the Radiological Concepts and Tactics and Integration Course (RCTIC), enhancing the VIPR Program's ability to plan and execute the "search, locate, and identify" phases of radiological and nuclear threat response. Each RCTIC iteration includes a capstone exercise to enhance and reinforce the course material.

Objective 4: Maintain and enhance programs to appropriately secure critical surface transportation physical and cyber infrastructure

Activity: Establish criteria to identify infrastructure that is most critical.

Key Accomplishments:

- TSA, in conjunction with DHS and industry stakeholders, identified critical infrastructure assets of national concern through the Top Transit Asset List (TTAL), which includes critical underwater tunnels, underground stations or tunnels, shared transportation facilities, and any other asset that would severely affect the overall system if lost or damaged. TSA began a comprehensive assessment of all 67 TTAL assets to verify/determine the status of security vulnerability, remediation efforts, and what additional security resources are necessary at each location through site visits, conference calls, and other outreach. In FY 2016, 45 TTAL assets were assessed, with the remaining 22 assets scheduled for assessment in FY 2017.
- Over $5.6 million was awarded to TTAL asset owners, publicly owned operators of public transportation systems, through the Transit Security Grant Program (TSGP) in 2016. Examples of funding priorities are mobile explosive screening and canine teams, vulnerability assessments and security plans, drills and exercises, and training. To date, more than $570 million has been provided for asset remediation efforts.
- TSA coordinated with the surface transportation industry to share data and information collected from the 10 TSA surface transportation test beds, encompassing all surface transportation modes.

Objective 5: Maintain and enhance programs to appropriately secure the physical and cyber components of critical mass transit and passenger rail infrastructure and systems

Activity: MTPR systems stakeholders continue to apply measures that mitigate security risks of the transportation network.

Key Accomplishments:

- MTPR stakeholders, transit police, FBI, and cybersecurity experts participated in the annual MTPR Security Roundtable. Industry continues to indicate that this forum provides valuable security information and insights.
- The American Public Transportation Association convened a Communications and Control Systems Recommended Practice Working Group meeting with industry and the DHS National Cybersecurity Communications and Integration Center (Industrial Control Systems-Cyber Emergency Response Teams) to review and discuss DHS incident response support capabilities for the Nation's top passenger rail agencies.

Industry indicated that they would like more cyber-related events; therefore, more cybersecurity-focused MTPR events are being scheduled for the remainder of calendar year 2017 and beyond.

- TSA maintained outreach to the mass transit and passenger rail transportation industry to provide data and information gleaned from five test beds encompassing mass transit and passenger rail.

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: Collaboration between TSA and industry on intelligence and information products, best practices, and protective measures occurs through daily interaction and engagement, as well as through formal structures, including the DHS-led Critical Infrastructure Partnership Advisory Council framework, Sector Coordinating Council, and other industry-centric organizations, such as the Mass Transit Policing and Security Peer Advisory Group that represents the top 26 high-risk MTPR systems across the United States, Canada, and the United Kingdom. TSA also strongly encourages the use of the "If You See Something, Say Something™" public awareness campaign. Similarly, TSA's "Not On My Watch" program is focused on the surface transportation community and is designed to make employees of surface transportation systems part of awareness programs intended to safeguard transportation systems against terrorism and other threats.

Objective 1: Maintain and enhance the means and mechanisms for receiving suspicious information reports from transit agencies, passenger rail operators, and personnel and for sharing timely and relevant information and intelligence between government agencies, and mass transit and passenger rail operators

Activity: Evaluate and improve the quality of intelligence and information products and the unclassified information delivery system provided to the mass transit and passenger rail owners and operators.

Key Accomplishments:

- TSA provided monthly reports analyzing "significant security concerns" made by railroads to comply with 49 C.F.R. part 1580 and provided quarterly reports with analysis of trends.
- MTPR stakeholders, transit police, FBI, and cybersecurity experts participated in the annual MTPR Security Roundtable. Physical and cybersecurity experts came together to inform and share their perspective on law enforcement and cybersecurity issues.
- The American Public Transportation Association convened a Communications and Control Systems Recommended Practice Working Group meeting with industry and the DHS National Cybersecurity Communications and Integration Center (Industrial Control Systems-Cyber Emergency Response Teams) to review and discuss DHS incident response support capabilities for the Nation's top passenger rail agencies.

Objective 2: Engage first responders and the public to understand community risks related to mass transit passenger rail infrastructure and services, to promote preparedness for security concerns, and to improve community resilience

Activity: Promote use of effective public awareness campaigns in communities served by mass transit and passenger rail operations.

Key Accomplishments:

- Facilitated 13 peer advisory group calls, scheduled monthly or event-driven, to discuss emerging threats, provide intelligence updates, security challenges overseas, and issues of national MTPR security concern.
- Held monthly transit industry information sharing teleconference calls to disseminate intelligence information and security program updates. These calls are open to the entire MTPR industry population.
- Planned and executed the MTPR Security and Emergency Management Roundtable in Phoenix, Arizona, which assembled law enforcement chiefs, security directors, and safety directors from the Nation's 60 largest MTPR agencies, including Amtrak.
- Issued 10 Security Awareness Messages (SAMs) during times of heightened alert or in response to terrorism events. These messages provide security information and awareness information that emphasize threat-specific existing security measures and/or recommend voluntary protective measures.
- Supported 10 Amtrak-lead Operation RAILSAFE activities, which were planned for the year. On average, RAILSAFE activities included over 170 agencies across 38 states, 1,200 personnel, and almost 200 stations per event.
- TSA funds the American Public Transportation Association to manage the Public Transportation Information Sharing and Analysis Center (PT-ISAC), which provides to its constituency a 24/7 Security Operating Capability for MTPR specific critical information/intelligence requirements for incidences, threats and vulnerabilities. It also disseminates the Transit and Rail Intelligence Awareness Daily Report.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

Overall Assessment: TSA continued to consider the privacy, civil liberties, and civil rights of individuals and entities in developing and implementing processes ensuring the freedom of movement of people and commerce.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy pursuant to applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishment: All field activities were evaluated to ascertain compliance with established laws, regulations, and policy.

Table 6: Freight Rail Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attack and enhance system resilience

Overall Assessment: Freight Rail (FR) federal security partners and industry stakeholders continue to sustain a risk-based security posture. Freight railroads continue to sustain the reductions in risk associated with the transportation of Rail Security-Sensitive Materials (RSSM) that have been achieved over the last decade. The application of risk-based priorities including planning, training, exercises, risk reducing practices, information sharing, community outreach, and critical infrastructure protection has enabled the freight railroads to reduce the risks to their operations and the national freight rail network.

Objective 1: Sustain effective security plans through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences

Activity: Develop security plans, periodically review, and update based on available information.

Key Accomplishment: 100 percent of railroads that transport RSSM[17] through High Threat Urban Areas[18] have security plans and contingency preparations to implement enhanced risk mitigating measures at elevated terrorism alert levels.

Objective 2: Provide effective training for railroad frontline employees

Activity: Conduct training of frontline employees to identify, prevent, deter, and respond to threats.

Key Accomplishments:

- Approximately 85,148 frontline employees of Class I railroads received or participated in security awareness training.
- TSA developed modal and Cyber Counterterrorism Guides in collaboration with industry stakeholders, as part of a cooperative effort to improve transportation system security and enhance the recognition of indicators of possible terrorist activity. Copies of the Freight Rail Counterterrorism Guide and Cyber Counterterrorism Guide were

[17] The group of 33 Class I railroads that transport RSSM through High Threat Urban Areas includes the 7 Class I railroads constitute approximately 90 percent of all railroad employees and 80 percent of the rail operating miles in the United States.

[18] There are 46 regulated High Threat Urban Areas.

provided to all of the Nation's freight railroads for their consideration. TSA received requests for additional guides and distributed over 11,000 Counterterrorism Guides to railroads. The Counterterrorism Guides were also provided to Transportation Security Inspectors for distribution to freight rail employees in the field.

- TSA distributed training and security awareness Digital Video Discs (DVD) and posters to government and external entities.
- Published the Security Training for Surface Transportation Employees Notice of Proposed Rulemaking and the Surface Transportation Vulnerability Assessments and Security Plans Advance Notice of Proposed Rulemaking with consideration given to Goal 3 intent and objectives during the draft/review processes.

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Railroads either conduct or participate in exercises designed to evaluate the preparedness for, and response to, security events.

Key Accomplishments:

- The Class I railroads conducted 248 exercises focused on preparedness to address general or specific threats and security-related incidents or contingencies.
- Facilitated the use of the Simulation Deck platform[19] during the Association of American Railroads annual security exercise. This platform added a real-world feel to the exercise by injecting simulated media (video, radio, blogs, and social media) into the exercise environment.
- Coordinated the participation of four railroads in the New Orleans Regional Intermodal Security Exercise.
- VIPR Personnel supported nine iterations of RCTIC, enhancing the VIPR Program's ability to plan and execute the "search, locate, and identify" phases of radiological and nuclear threat response. Each RCTIC iteration includes a capstone exercise to enhance and reinforce the course material.

Objective 4: Maintain and enhance programs to appropriately secure critical railroad physical and cyber infrastructure

Activity: Establish or update criteria to identify which infrastructure is most critical, and enhance programs to appropriately secure railroad critical infrastructure.

Key Accomplishments:

- TSA developed and implemented a database to house data collected on 288 bridge and tunnel security assessments. This database will allow TSA to do further analysis as

[19] Simulation Deck is a web-based platform designed for use in crisis simulations (exercises) that emulates a variety of social media and news outlets. It is one of the services available to support the TSA I-STEP. (http://simulationdeck.com/)

well as follow up assessments of infrastructure assets with significance to the operation of the national rail network.

- Distributed reports of highway bridge and tunnel assessments prepared by the U.S. Army Corps of Engineers to the owners of critical railroad infrastructure to inform their respective Engineering Departments of the vulnerabilities of structural components of bridges and tunnels.
- Completed the installation of surveillance and monitoring equipment on two freight rail bridges as part of the surface infrastructure test bed program. This provides real-time situational awareness, even from remote unattended sites, through secure connectivity and sophisticated displays.
- Continued to improve three test beds, including freight rail bridges and the infrastructure protection test bed in Northern New Jersey.
- Continued outreach to the surface transportation industry to provide data and information gleaned from the freight rail test beds.
- Instituted a new Concept of Operations to enhance and focus risk-based planning and deployment of VIPR teams in an unpredictable and random manner in the freight rail domain.

Objective 5: Maintain operational procedures for reducing the risk associated with the transportation of passengers and materials of concern

Activity: Railroad carriers and shippers and receivers of RSSM continue to apply measures that mitigate security risks of the transportation of these materials in High-Threat Urban Areas.

Key Accomplishments:

- The railroads, as required by 49 C.F.R. 1580.107, continued to apply operational measures that reduce the vulnerability of RSSM transiting High-Threat Urban Areas (HTUA). These measures include the inspection of RSSM cars and the secure exchange of custody at points of origin, interchange with other railroads, and points of delivery. TSA conducted 2,467 inspections for compliance with the RSSM chain of custody regulations. TSA also monitors the attendance of rail tank cars containing Toxic Inhalation Hazard materials being temporarily held or stopped in HTUAs. TSA conducted 11,624 observations of toxic hazard tank car attendance.
- The results of these observations and inspections show that the railroad industry had an attendance rate of 98.71 percent and a compliance rate of 99.75 percent.
- Class I railroads conducted exercises focused on preparedness to address risk to the tracks, which are typically used by both freight rail companies and passenger rail services.

Goal 2: Enhance effective domain awareness of transportation systems and threats

<u>Overall Assessment</u>: TSA and its federal partners worked with industry organizations, such as the Railway Alert Network, to ensure rail security coordinators were provided with a variety of informational products to provide continuous awareness and assist in strategic and tactical planning for existing and emerging threats. Many of these products serve as the basis for educational and training materials for frontline employees. TSA routinely provides information on both kinetic and cyber threats to the railroad operators. TSA also regularly participates in the Association of American Railroads Rail Security Working Committee meetings.

Objective 1: Maintain and enhance mechanisms for information and intelligence sharing between the railroad industry and government

Activity: Ensure delivery of timely, meaningful, and actionable intelligence and security information products to rail security coordinators.

Key Accomplishments:

- TSA distributed more than 80 separate security information and intelligence products to designated rail security coordinators and security partners, including those produced by TSA and other DHS components and federal agencies. Examples of information and intelligence products include TSA Modal Threat Assessments, SAMs, Transportation Intelligence Notes, and DHS Joint Intelligence Bulletins.
- TSA provided monthly reports analyzing "significant security concerns" made by railroads to comply with 49 C.F.R. part 1580 and provided quarterly reports with trend analysis.
- Maintained and managed a database of Rail Security Coordinators for freight railroads, hazardous materials shippers, and hazardous materials receivers. Continued to provide data and information gleaned from the three freight rail test beds to the freight rail industry.

Objective 2: Engage with first responders and the public to provide awareness of security concerns associated with railroad operations to promote situational security awareness and preparedness

Activity: Conduct activities and information-sharing with law enforcement, public safety, and the general public that improve security awareness and understanding of the railroad's operations.

Key Accomplishment: Railroads had 5,176 security awareness engagements, which are reports of possible suspicious activity and interactions with law enforcement, emergency responders, and the public in their operating areas.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

Overall Assessment: TSA continues to consider the privacy, civil liberties, and civil rights of individuals and corporations in developing and implementing processes ensuring the freedom of movement of people and commerce.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishment: All field activities were evaluated to ascertain compliance with established laws, regulations, and policy.

Table 7: Highway and Motor Carrier Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience

Overall Assessment: TSA collaborates with Highway and Motor Carrier (HMC) owners and operators to identify risks to critical systems and services, and aid in implementing risk-mitigating policies and programs to address gaps that may exist. BASE assessments of the largest trucking carriers, motorcoach operators, and pupil transportation operations further help stakeholders to understand and close security gaps in their systems.
Exercise programs are essential to assist operators in directing their resources and efforts toward effective risk reduction. TSA facilitates I-STEP exercises to help HMC entities test and evaluate their security plans. In addition, EXIS, which is a TSA-sponsored online exercise tool, guides government and industry users through the exercise planning process and provides resources to design, document, and evaluate exercises for all transportation modes. Training programs, including the First Observer Plus ™ and Counterterrorism Guides, aid in informing a large percentage of the HMC employee population of security responsibilities and actions to identify and report security concerns.

Objective 1: Sustain effective security plans through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences

Activity: Develop vulnerability assessment and security planning guidance and tools for use by operators.

Key Accomplishments:

- Completed 87 BASE assessments that provide a random sample of operators' voluntary implementation of recommended security measures. Due to the mode's large number of operators, TSA conducted random inspections to identify progress and need-to-improve areas in security plans.
- Completed a six-year U.S. Army Corps of Engineers significant bridge and tunnel vulnerability assessment program. Issued comprehensive documents identifying both structural and operational vulnerabilities of typical designs applicable to 95 percent of all bridges and 100 percent of all tunnels. This work is accessible to state and local

authorities as a resource not only for hardening existing structures, but also for enhancing the secure design of new structures.

Objective 2: Provide effective training for highway frontline employees

Activity: Develop training resources and tools for use by operators based on identified needs (i.e., vulnerabilities, threat indicators, and threat incident response protocols).

Key Accomplishments:

- Published the HMC Toolkit providing operators with potential threats and mitigating actions.
- Published the First Observer Plus™ security awareness training program.
- Issued a Notice of Proposed Rulemaking pursuant to congressional mandate dealing with security awareness training for frontline employees in Over-the-Road Bus, freight rail, and MTPR.
- Compiled and released to stakeholder's industry practices on conducting vulnerability assessments, security training, and threat assessments.
- Provided HMC Counterterrorism Guides and Cyber Counterterrorism Guides to industry stakeholders as part of a cooperative effort to improve HMC security.

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Use exercise program to evaluate the resilience of over-the-road bus operations to terrorist attack.

Key Accomplishment: TSA completed six I-STEP exercises in Baltimore, Maryland; Tucson, Arizona; and Kansas City, Missouri. In addition, TSA rolled out the EXIS in-person to HMC systems in three cities: Minneapolis, Minnesota; Cincinnati, Ohio; and New Martinsville, West Virginia. Based on these exercises, best practices and lessons learned were developed.

Objective 4: Maintain and enhance programs to appropriately secure critical physical and cyber infrastructure

Activity: Coordination and collaboration with industry to identify both physical and cyber vulnerabilities.

Key Accomplishments:

- Provided cybersecurity toolkit and other cyber security information throughout the HMC stakeholder community.
- Completed a six-year U.S. Army Corps of Engineers significant bridge and tunnel vulnerability assessment program. Issued comprehensive documents identifying both structural and operational vulnerabilities of designs of 95 percent of all bridges and 100 percent of all tunnels.

- Distributed comprehensive documents generated by Corps of Engineers project to all state homeland security directors.
- Distributed comprehensive documents generated by Corps of Engineers project to Transportation Research Board within the National Academy of Sciences for use as guidance in construction of new bridges and tunnels.

Objective 5: Maintain operational procedures for reducing the risk associated with the transportation of passengers and materials of concern

Activity: Continuous development of options to mitigate potential threats to highway and motor carrier operators.

Key Accomplishment: Provided relevant counterterrorism information to stakeholders, and security tools and resources to mitigate potential threats (i.e., I-STEP exercises, Counterterrorism guides).

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: TSA continued to develop highly cooperative stakeholder relationships by expanding domain awareness training and information sharing activities. Similarly, TSA and its partners implemented new awareness training tools and implemented more informative messaging systems to ensure HMC stakeholders are aware of the most current threat information. TSA routinely provides information on both kinetic and cyber threats to the HMC industries. TSA also routinely participates in industry events and on security committees to raise the level of awareness and provide security tools and resources to private entities for implementation.

Objective 1: Maintain and enhance the mechanisms for information and intelligence sharing between the highway and motor carrier industry and government

Activity: Evaluate and improve the quality of intelligence and information products and the unclassified information delivery system provided to the highway and motor carrier operators and infrastructure owners.

Key Accomplishments:

- Initiated quarterly conference calls providing stakeholders with current intel and threat briefs, updates on programs and policies, and an opportunity for stakeholder questions and comments.
- Issued 10 SAMs to industry covering peak travel periods (e.g., Memorial Day, July Fourth, Thanksgiving, and Christmas/New Year's). In addition, SAMs were issued on anniversary dates of symbolic importance such as 9/11, London subway bombings (July 7), and the Madrid train bombings (March 11).

- Conducted stakeholder follow-up calls with all modal stakeholders in the wake of significant terrorist attacks overseas. Each call contained current threat and technique analysis and opportunity for stakeholder questions and input.
- Sponsored the delivery of daily reports to stakeholders through the Public Transit-Surface Transportation-Over-The-Road-Bus Information Sharing and Analysis Center.

Objective 2: Engage with first responders and the public to provide awareness of security concerns associated with highway operations, and to promote situational and security awareness, and preparedness. Use the TSA Intermodal Security Training and Exercise Program and Exercise Information System programs to identify lessons learned and promote risk reduction activities throughout the highway and motor carrier landscape.

Activity: Conduct effective exercises with both private and public partners in high-risk areas by employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience.

Key Accomplishments:

- Planned, budgeted and executed eight I-STEP exercises with local, state, and federal law enforcement and first responder entities.
- Provided security awareness and TSA security initiative updates at more than 15 public/private stakeholder events/calls.
- Distributed comprehensive documents generated by Corps of Engineers project to all state homeland security directors and state departments of transportation homeland security officers.
- Distributed comprehensive documents generated by Corps of Engineers project to the Transportation Research Board within the National Academy of Sciences for use as guidance in construction of new bridges and tunnels.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: HMC stakeholders responded well to voluntary participation in BASE assessments with the assurance that findings and recommendations are closely held under Sensitive Security Information standards or, where appropriate, classified information policies. BASE assessments and U.S. Army Corp of Engineers structural visits are scheduled to ensure the flow of commerce is not interrupted.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishment: All field activities were evaluated to ascertain compliance with established laws, regulations, and policy.

Table 8: Pipeline Progress Assessment

Goal 1: Manage risks of terrorist attacks and enhance systems resilience

Overall Assessment: TSA worked closely with government and industry stakeholders to secure the Nation's pipeline systems from terrorist attacks largely through voluntary security program implementation, robust industry engagement, and collaborative technology test beds. TSA and the pipeline industry security partners continued to use the Critical Facility Security Review (CFSR) and Corporate Security Review (CSR) programs to assess risk throughout the operating environment of the top 100 critical pipeline systems. Both programs highlight stakeholder opportunities to implement the 2011 TSA Pipeline Security Guidelines and share industry smart/best practices. Additionally, plans designed to enhance TSA CFSR and CSR delivery reached fruition as TSA secured a new, five-year CFSR contract and initiated plans to expand the CSR program. TSA provided stakeholders additional opportunity to implement the NIST CyberSecurity Framework throughout the security operations environment by providing framework overviews and links in pipeline industry specific Counterterrorism Guides.

Objective 1: Maintain operational protocols for reducing the risk associated with the transmission through pipelines of natural gas, hazardous liquids, and materials categorized as toxic inhalation hazards

Activity: Strategically integrate TSA Pipeline Security Guidelines throughout the security operations environment of industry partners owning and operating our Nation's most critical natural gas and hazardous liquid pipeline systems by continued engagement of the CSR and CFSR programs and related processes.

Key Accomplishments:

- Integrated TSA Pipeline Security Guidelines throughout the industry's security operations environment with continued collaborative engagement through the CSR and CFSR programs and process with members of the top 100 critical pipeline system stakeholders.
- Established baselines for each program used to measure future guidelines adoption by industry.
- Continued two pipeline site security technology test beds, including advanced infrastructure protection technologies.
- Instituted a new Concept of Operations to enhance and focus risk-based planning and deployment of VIPR teams in an unpredictable and random manner in the pipeline transportation domain.

Objective 2: Enhance cyber-security of the pipeline critical infrastructure

Activity: Conduct outreach with pipeline industry stakeholders on the voluntary implementation of the principles and best practices of risk management through the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Key Accomplishments:

- Established a methodology to deliver the NIST Cyber-Security Framework to industry via links included in the Pipeline Counterterrorism Guides.
- Established an industry Framework implementation baseline to measure future industry adoption of the Framework.

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: TSA's strong stakeholder engagement program remained focused on the delivery of value-added situational awareness messages, intelligence briefings, and other information sharing products through a trusted, effective network consisting of pipeline industry and government partners.

In addition, TSA uses these same information sharing networks to:

- Coordinate and deliver training;
- Coordinate security exercises, assessments and reviews;
- Deliver industry-specific training materials such as Pipeline Counterterrorism Guides, DVDs, and CDs;
- Share Smart/Best Practices; and
- Share security guidelines.

As prescribed in the DHS National Infrastructure Protection Plan, TSA relies on the Critical Infrastructure Partnership Advisory Council process to facilitate government and industry information and intelligence sharing and security planning, coordination, and execution. Under the Critical Infrastructure Partnership Advisory Council, the Pipeline Sector Coordinating Council and Government Coordinating Council consider the entire range of intelligence and information sharing venues, pipeline security strategies, policies, activities, capability gaps, technology initiatives, and related issues when developing modal specific strategy, plans, and initiatives. Additionally, TSA continues to participate in Energy Government Coordinating Council meetings and Oil and Natural Gas Government Coordinating Council/Sector Coordinating Council meetings. TSA continued to seek opportunities to further develop relationships with foreign government security counterparts, with particular emphasis on Canada and Mexico.

Objective 1: Enhance the means to share information and intelligence between the pipeline industry and government

Activities:

- Assess opportunities for enhanced information sharing processes with the natural gas and hazardous liquid pipeline community through industry developed activities such as Information Sharing & Analysis Centers.
- Deliver timely, meaningful, and actionable security information products to pipeline industry security coordinators.

Key Accomplishments:

- TSA provided seven unclassified threat briefings to industry representatives at monthly pipeline security conference calls.
- TSA developed, published, and distributed industry specific Counterterrorism Guides for all industry stakeholders and established a baseline to measure and improve distribution to the top 100 critical pipeline systems.
- TSA continued outreach to the pipeline industry, providing data and information gleaned from the two pipeline test beds.

Objective 2: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Test and improve resilience to terrorist attack by collaborating with stakeholders to develop Pipeline Industry specific I-STEP exercises featuring key DHS/TSA risk reduction areas of consideration such as supply chain disruption.

Key Accomplishments:

- TSA collaborated with industry to plan, develop, and deliver two I-STEP exercises based on overarching TSA risk mitigation and resilience strategies and plans. VIPR Personnel supported nine iterations of the RCTIC, enhancing the VIPR Program's ability to plan and execute the "search, locate, and identify" phases of radiological and nuclear threat response. Each RCTIC iteration includes a capstone exercise to enhance and reinforce the course material.

Objective 3: Work with industry stakeholders and encourage them to engage with first responders and the public to understand community concerns and resilience needs, to provide awareness of pipeline security issues, and to promote system preparedness and resilience

Activity: Maintain and enhance commitment to sustained engagement with first responders, customers and the public to provide awareness of security concerns and preparedness measures.

Key Accomplishments:

- TSA collaborated with industry to plan, develop, and deliver two I-STEP exercises featuring first responder participation.
- Developed First Observer Plus ™ training and delivered to industry stakeholders.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: TSA continued to consider the privacy, civil liberties, and civil rights of individuals and corporations in developing and implementing processes ensuring the freedom of movement of people and commerce. All related pipeline risk-based security initiatives and activities were evaluated to ensure compliance with established standards and policy.

Objective: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishment: Considered the Goal 3 Objective and Activity in the updated TSA Pipeline Security Guidelines, which were developed collaboratively with industry.

D. Intermodal

The Intermodal Security Subsector covers the transportation elements of the global supply chain and the delivery of goods from origin to destination by multi-modal postal and parcel shipping services. The global supply chain consists of a dense network of routes and carriers operating efficiently to provide time-sensitive deliveries. Threats to intermodal transportation links of the supply chain are the same as those for the individual modes serving the supply chain. The threats also include the potential delivery of explosives, dangerous chemicals, or biological agents to specific targets. While the direct consequences of attacks on intermodal transportation systems may be limited, the indirect costs of attack-related disruptions could have significant and lasting effects, particularly where shipping options are limited.

Table 9: Intermodal Progress Assessment

Goal 1: Enhance resilience of the global transportation supply chain system

Overall Assessment: The sector continues to collaborate with industry stakeholders and security partners on supply chain issues and innovative approaches to security. TSA participated in a policy development process with industry engagement and the Compliance Security Enhancement Through Testing Program to enhance industry compliance through measures other than penalties. In addition, the subsector coordinated the U.S. and international positions on cargo technological standards, supply chain security, and advance cargo information with international cargo security working groups, such as the International Civil Aviation Organization's Aviation Security Panel.

Objective 1: Reduce systemic risk of a supply chain disruption prior to a potential nationally-significant event by using layered risk management principles
Objective 2: Improve capacities to effectively collect, protect, analyze, and share supply chain information among stakeholders, and strengthen and grow stakeholder partnerships and collaboration
Objective 3: Ensure orderly resumption of commerce following a large-scale disruption

Activities:

- Assure compliance with international security protocols such as the International Ship and Port Facility Security Code.
- Implement the International Port Security Program to assess the effectiveness of anti-terrorism measures in foreign ports, build security capacity where gaps exist, and impose conditions of entry on vessels arriving in the United States from ports with substandard security.
- Conduct exercises of the National Response Framework, the Response Federal Interagency Operational Plan, and other related all hazards and security incident response plans to enhance resumption of trade following a large-scale disruption.

Key Accomplishments:

- Conducted DHS-led regional assessments using the Regional Resilience Assessment Program to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen infrastructure resilience. Key findings concentrate on regionally significant issues and present options to enhance resilience.
- The USCG conducted 5,937 MTSA facility inspections, which aim to prevent maritime transportation security incidents and marine casualties resulting from malicious acts, accidents, or acts of nature against waterfront facilities.
- I-STEP engaged with over 75 stakeholder groups to conduct multiple intermodal security exercises, resulting in after-action reports and development of industry practices.
- Instituted a new Concept of Operations to enhance and focus risk-based planning and deployment of VIPR teams in an unpredictable and random manner in the intermodal domain.

Goal 2: Enhance the efficient and secure movement of goods

<u>Overall Assessment</u>: The Air Cargo Advance Screening (ACAS) Pilot Program, initiated in 2010, allows TSA inspectors to work with CBP officers to identify high-risk air cargo shipments, facilitating targeted, enhanced screening prior to loading on board U.S.-bound aircraft. TSA and CBP held multiple meetings with industry stakeholders to discuss requirements, regulations, lessons-learned and progress toward implementation. TSA and

CBP continue to jointly develop a rulemaking to replace the ACAS Pilot Program with a permanent ACAS requirement.

Objective 1: Mitigate and manage risks as early as possible in the global supply chain networks to promote the efficient flow of commerce

Activities:

- Apply risk segmentation methods to focus security resources on higher risk cargos (Automated Targeting System, Automated Manifest System, Air Cargo Advance Screening, and Customs-Trade Partnership Against Terrorism[20]).
- Implement advance notice of arrival protocols including CBP's 24-Hour Advanced Manifest Rule and the USCG's 96-Hour Advance Notice of Arrival to identify higher risk cargo movements for enhanced security review.
- Enhance Air Cargo Security Programs: require shippers, air forwarders, independent facilities and airlines to screen cargo before it is loaded aboard aircraft.

Key Accomplishments:

- The ACAS pilot was extended through July 26, 2017. This action was taken to allow additional time for the two lead agencies, CBP and TSA, to develop a rulemaking.
- TSA enrolled approximately 505,000 workers in the TWIC® Program[21], for a program total of 3.6 million, providing a security threat assessment and tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the MTSA, and all USCG credentialed merchant mariners.
- CBP prescreened over 80 percent of all maritime containerized cargo imported into the United States at 58 operational Container Security Initiative ports.
- Conducted security threat assessments on more than 250,000 truck drivers, vetting applicants against criminal, immigration, and intelligence databases for Hazardous Materials Endorsements issued by State motor vehicle agencies, for a total enrollment of 3 million. Of those vetted over the lifetime of the program, 1.3 million individuals have an active security threat assessment.
- Enrolled approximately 273,000 people in the Hazardous Materials Endorsement Threat Assessment Program for a total enrollment of 3 million.
- The USCG conducted 5,937 MTSA facility inspections that aim to prevent maritime transportation security incidents and marine casualties resulting from malicious acts, accidents, or acts of nature against waterfront facilities.

[20] Additional information on these program is available on https://www.dhs.gov.

[21] Required by the Maritime Transportation Security Act (Pub.L. 107–295) for workers who need unescorted access to secure areas of the nation's maritime facilities and vessels.

Objective 2: Enhance implementation of global supply chain-related standards, best practices, and guidelines and regulations allowing stakeholders to realize efficiencies while maintaining acceptable levels of security

Activity: Implement Customs-Trade Partnership Against Terrorism to improve the security of private companies' supply chains with respect to terrorism.

Key Accomplishments:

- Used Pre-Loading Advance Cargo Information to examine the application of advanced cargo information and as a platform for dialogue among pilot program participants and between regulators and industry.
- Collaborated with the International Civil Aviation Organization Aviation Security Panel Working Group on Air Cargo on the concept of best practices or similar material that may be appropriate for the International Civil Aviation Organization to develop. This material would include the use of Pre-Loading Advance Cargo Information for aviation security purposes for those states considering using air cargo information for targeting.

Objective 3: Improve situational awareness of terrorist threats to the global supply chain

Activity: Work with the Office of the Director of National Intelligence, the Department of Defense, and industry to develop cyber risk assessment capabilities that can address global supply chain security.

Key Accomplishments:

- Continued to work closely with industry to encourage adoption of the NIST Cybersecurity Framework and issued the Transportation Systems Sector Cybersecurity Framework Implementation Guidance document.
- Strengthened cybersecurity information sharing via the Aviation Government Coordinating Council and Sector Coordinating Council, including its Cybersecurity Working Group[22].
- Participated in the Aviation Cybersecurity Initiative, a DHS National Protection and Programs Directorate-led interagency working group that is identifying potential cybersecurity vulnerabilities in aviation and developing potential solutions to mitigate any identified vulnerabilities.
- Participated in a DHS Cybersecurity Integrated Project Team process researching "High-Priority Technology Solutions."
- Completed and deployed the Automated Commercial Environment, which is CBP's primary system (i.e., single window) through which the trade community reports

[22] The Critical Infrastructure Partnership Advisory Council provides the operational framework for the sector partnership structure and is aligned with the National Infrastructure Protection Plan and Presidential Policy Directive.

imports and exports and the government determines admissibility. Through the Automated Commercial Environment manual processes are streamlined and automated, paper is being eliminated and the international trade community is able to more easily and efficiently comply with U.S. laws and regulations.

Objective 4: Improve industry involvement in the global supply chain Research and Development process to improve security of goods in transit and minimize delays

Activity: Improve industry participation in development of the Cargo and Supply Chain R&D Plan.

Key Accomplishments:

- The joint Transportation Sector R&D Working Group and DHS Integrated Project Team on Aviation Security identified capability gaps and recommended priority R&D projects for consideration by DOT and by DHS Science and Technology Directorate.
- The joint Surface Transportation Systems R&D Working Group, including DHS, DOT, and public and private partners, identified security capability gaps in the surface modes of transportation, which serve as a basis for developing R&D project requirements for consideration by the funding organization.
- Continued to enhance industry participation in the development of the National Strategy For Transportation Security, and in support of the DHS Directorates for Science and Technology, and National Protection and Programs, the National R&D Plan, and the National Infrastructure Protection Plan.

Objective 5: Enhance the security of critical infrastructure and conveyances in order to protect the supply chain and nodes against terrorist attacks

Activities: See activities in the 2016 NSTS Modal Security Plans.

Key Accomplishments:

- Developed and distributed an Insider Threat awareness video for aviation workers.
- Maintained robust formally established marketplace-based technology assessments and formally established test beds in collaboration with transportation operators.

Table 10: Postal and Shipping Progress Assessment

Goal 1: Manage risks to the P&S Subsector and enhance system resilience

Overall Assessment: The Postal & Shipping (P&S) Subsector continues to remain vigilant to ensure the continuity of operations, ease of use, and public confidence by creating a multi-layered security posture that integrates public and private partners and protective measures to deny adversaries the ability to exploit the subsector and its customers. There have been no significant events to impact the subsector.

Objective 1: Improve deterrence and response to a national or regional terrorist emergency affecting the P&S Subsector

Activity: Improve risk assessment processes.

Key Accomplishments:

- Conducted 1,007 postal facility[23] reviews by Security Control Officers, Physical Security Specialists, and Postal Inspection Service employees utilizing the Vulnerability Risk Assessment Tool, a comprehensive, risk-based model that identifies security deficiencies.
- Conducted five reviews at airports with international service centers to assess procedures, internal and external controls and security measures used in the handling of U.S. mail.
- Inspectors received the Hazardous Material Training and Improvised Explosive Device Recognition and Response Course to recognize the components of a mail bomb device using portable equipment. This training was applied at the 2016 Democratic and Republican National Conventions, where over 39,000 mail pieces were screened.

Objective 2: Minimize the risk of unauthorized individuals gaining access into secured areas

Activity: Expand voluntary use of best-practice security protocols.

Key Accomplishments:

- Developed best-practice guides based on airport reviews that assess procedures, internal and external controls and security measures used in the handling of U.S. mail.
- Expanded the use of closed-circuit television and electronic access control to stations to reduce vulnerabilities and mitigate risks.

Goal 2: Enhance effective domain awareness of P&S systems and threats

Overall Assessment: The P&S Subsector ensures continuity of operations by providing incident-reporting mechanisms and awareness/outreach programs with law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the subsector. These activities ensure timely, relevant, and accurate threat reporting from law enforcement and intelligence communities to key decision makers in the sector in order to implement appropriate threat-based security measures and risk management programs. The community is linked through the Homeland Security Information Network.

Objective 1: Improve awareness of cross sector interdependencies

[23] A postal facility is defined as any type of facility (information technology, personnel office, mail center) with U.S. Postal Service employees or contractors. There are 31,606 postal facility locations, including 461 processing centers that process large amounts of mail.

Activities:

- Partner with industry and the Intelligence Community to facilitate threat awareness. Use the Homeland Security Information Network to communicate with the P&S community to retrieve and update information and intelligence. Work to develop a communications procedure for routine and incident-specific information sharing.
- Assess interdependencies of other sectors relying on P&S.

Key Accomplishment: TSA had no significant accomplishments toward these objectives in 2016. Developing a communications procedure for routine and incident-specific information sharing is not feasible at this time because each entity has its own specific proprietary intelligence and reporting network. No interdependency assessment was conducted during this period.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: The P&S subsector processed 154.2 billion letters and parcels and delivered them to more than 155 million addresses in every state, city, and town in the country. The U.S. Postal Inspection Service provided security for these mail pieces from their entry into the postal network to their destinations. Federal law forbids tampering with the mail; only the person to whom a mail piece is addressed may open it. Postal Inspectors have the investigative jurisdiction in cases where mail delivery is interrupted by theft, riffling, obstruction, or destruction. Through enforcement measures and educational programs, the Inspection Service is thwarting crime and keeping the mail safe and secure.

Objective 1: Minimize the security risks and delays in freight movement and reduce potential for adverse privacy, civil rights and civil liberty impacts of security policies

Activity: Enhance continuity of operations plans to ensure the Sector identifies and protects privacy, civil rights and civil liberties in the free movement of parcels to intended recipients.

Key Accomplishment: The U.S. Postal Service established a website designed to educate and assist customers with scams and mail fraud. The Consumer Alert News Network also broadcasts segments on 120 television stations alerting the public to mail fraud and other postal crimes.

Appendix A: Acronym List

Acronym	Definition
ACAS	Air Cargo Advance Screening
ADIAC	Aviation Domain Intelligence Integration and Analysis Cell
BASE	Baseline Assessment for Security Enhancements
CBP	U.S. Customs and Border Protection
CFSR	Critical Facility Security Review
CIPAC	Critical Infrastructure Partnership Advisory Council
CSR	Corporate Security Review
CT	Counter Terrorism
DHS	Department of Homeland Security
DOT	Department of Transportation
DVD	Digital Video Disc
ETD	Explosive Trace Detection
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FR	Freight Rail
GCC	Government Coordinating Council
HMC	Highway and Motor Carrier
ICAO	International Civil Aviation Committee
I-STEP	Intermodal Security Training and Exercise Program
MTPR	Mass Transit and Passenger Rail
MTS	Maritime Transportation Security
MTSA	Maritime Transportation Security Act
NIST	National Institute of Standards and Technology
NSTS	National Strategy for Transportation Security
ODNI	Office of the Director of National Intelligence
P&S	Postal and Shipping
PT-ISAC	Transit and Rail Intelligence Awareness Daily Report and Analysis Center
R&D	Research and Development
RAILSAFE	Regional Alliance Including Local, State, and Federal Efforts
RCTIC	Radiological Nuclear Detection Concepts, Tactics and Integration Course
RSSM	Rail Security-Sensitive Materials
SAM	Security Awareness Message
SCC	Sector Coordinating Council
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSGP	Transportation Security Grant Program

TSO	Transportation Security Officer
TTAL	Top Transit Asset List
TWIC®	Transportation Worker Identification Credential
USCG	United States Coast Guard
VIPR	Visible Intermodal Prevention and Response

Appendix B: Legislative Language: Annual Reporting Requirements

The Annual Report on Transportation Security covers four annual reporting requirements including implementation of the National Strategy for Transportation Security, the Transportation Systems Sector-Specific Plan, and other statutory requirements, as detailed below, to achieve efficiency and deliver a coordinated message to the White House and Congress. Appendix C provides a cross-walk showing how requirements are addressed this report. This report satisfies the following reporting requirements:

1. **Annual Periodic Progress Report on the National Strategy for Transportation Security: 49 U.S.C. § 114(s)(4)(C):**

   Periodic progress report –

   (i) Requirement for report. - Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, United States Code, the Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

   (ii) Content. - Each progress report submitted under this subparagraph shall include, at a minimum, the following:

   (I) Recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

   (II) An accounting of all grants for transportation security, including grants and contracts for research and development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the goals of the National Strategy for Transportation Security.

   (III) An accounting of all –

   (aa) funds requested in the President's budget submitted pursuant to section 1105 of title 31 for the most recent fiscal year for transportation security, by mode;

   (bb) personnel working on transportation security by mode, including the number of contractors; and,

   (cc) information on the turnover in the previous year of senior staff of the Department of Homeland Security, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department.

2. **Annual Report on Transportation Security: 49 U.S.C. § 44938(a):**
   (a) Submit to Congress a report on transportation security with recommendations the Secretary considers appropriate. The report shall include—
   (1) an assessment of trends and developments in terrorist activities, methods and other threats to transportation;
   (2) an evaluation of deployment of explosive detection devices;
   (3) recommendations for research, engineering and development activities related to transportation security, with exceptions as noted in statute;
   (4) identification and evaluation of cooperative efforts with other Federal entities;
   (5) an evaluation of cooperation with foreign authorities;
   (6) the status of the extent to which the recommendations of the President's Commission on Aviation Security and Terrorism have been carried out and the reasons for any delay in carrying out those recommendations;
   (7) a summary of the activities of the Assistant Administrator for Intelligence & Analysis;
   (8) financial and staffing requirements of the Assistant Administrator for Intelligence & Analysis;
   (9) assessment of financial and staffing requirements, and attainment of existing staffing goals, for carrying out duties and powers of the TSA Administrator related to security; and
   (10) appropriate legislative and regulatory recommendations.

3. **Annual Update on Enhanced Security Measures:** as required by Section 109(b) of the Aviation and Transportation Security Act (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296.

4. **Annual Report on the National Strategy for Public Transportation Security:** 6 U.S.C. § 1141:
   (a) Annual report to Congress
   (1) In general
   Not later than March 31 of each year, the Secretary shall submit a report, containing the information described in paragraph (2), to the appropriate congressional committees.
   (2) Contents
   The report submitted under paragraph (1) shall include—
   (A) a description of the implementation of the provisions of this subchapter;
   (B) the amount of funds appropriated to carry out the provisions of this subchapter that have not been expended or obligated;
   (C) the National Strategy for Public Transportation Security required under section 1133 of this title;
   (D) an estimate of the cost to implement the National Strategy for Public Transportation Security which shall break out the aggregated total cost of needed capital and operational security improvements for fiscal years 2008–2018; and

(E) the state of public transportation security in the United States, which shall include detailing the status of security assessments, the progress being made around the country in developing prioritized lists of security improvements necessary to make public transportation facilities and passengers more secure, the progress being made by agencies in developing security plans and how those plans differ from the security assessments and a prioritized list of security improvements being compiled by other agencies, as well as a random sample of an equal number of large- and small-scale projects currently underway.

(3) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

5. **Annual Report on the National Strategy for Railroad Transportation Security:**

6 U.S.C. § 1161

(e) Report

(1) Contents

Not later than 1 year after August 3, 2007, the Secretary shall transmit to the appropriate congressional committees a report containing—

(A) the assessment and the National Strategy required by this section; and § 1162 TITLE 6—DOMESTIC SECURITY Page 2561 So in original. The word ‘‘to’’ probably should not appear.

(B) an estimate of the cost to implement the National Strategy.

(2) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate
or necessary.

(f) Annual updates

Consistent with the requirements of section 114(t) 1 of title 49, the Secretary shall update the assessment and National Strategy each year and transmit a report, which may be submitted in both classified and redacted formats, to the appropriate congressional committees containing the updated assessment and recommendations.

Appendix C: Reporting Requirement Cross-walk

Requirement	Year	Due	Included in this Report	Notes
Annual Periodic Progress Report on the National Strategy for Transportation Security: 49 U.S.C. § 114(s)(4)(C)	December 14, 2004 – PL 108-458 Intelligence Reform & Terrorism Prevention Act	1-Mar[24]	--	
(i) Assess progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.			Yes	Included in Tables 3 - 10
(I) Recommendations for improving and implementing the NSTS and transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.			No	Addressed in NSTS, Section III of each modal plan
(II) An accounting of all grants for transportation security, including grants & contracts for research & development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the NSTS goals			No	FEMA manages and reports on Homeland Security Grant Programs (https://www.fema.gov/fiscal-year-2016-homeland-security-grant-program)

[24] Annually in conjunction with the submission of the budget to Congress under section 1105(a)("On or after the first Monday in January but not later than the first Monday in February of each year…")

Requirement	Year	Due	Included in this Report	Notes
(III) Accounting of all –			--	
(aa) funds requested in the President's budget submitted for the most recent fiscal year for transportation security, by mode;			No	2016 Budget-In-Brief, page 72 (https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf)
(bb) personnel working on transportation security by mode, including the number of contractors; and,			No	FY 2016 Congressional Budget Justification (https://www.dhs.gov/publication/congressional-budget-justification-fy-2016)
(cc) information on the turnover in the previous year of senior staff of the DHS, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department.			No	FY 2016 Congressional Budget Justification (https://www.dhs.gov/publication/congressional-budget-justification-fy-2016)
Annual Report on Transportation Security: 49 U.S.C. § 44938(a)	November 16, 1990 - PL 101-604 Aviation Security Improvement Act of 1990	31-Dec	--	
(1) assessment of trends and developments in terrorist activities, methods, and other threats to transportation;			No	Included in NSTS Section II Sector Risk Profile. Also developed in Transportation Sector Security Risk Assessment (TSSRA).

Requirement	Year	Due	Included in this Report	Notes
(2) evaluation of deployment of explosive detection devices;			No	See Electronic Baggage Screening Program, established by Congressional mandate for screening of all passenger checked baggage for concealed explosives (https://www.tsa.gov/for-industry/electronic-baggage-screening).
(3) recommendations for research, engineering, and development activities related to transportation security, with exceptions as noted in statute;			No	Included in Transportation Security Acquisitions Reform Act Strategic 5-year Technology Investment Plan
(4) identification and evaluation of cooperative efforts with other federal entities			No	Addressed in NSTS, Section VII
(5) evaluation of cooperation with foreign authorities;			No	Addressed in NSTS, Section VII
(6) status of the extent to which the recommendations of the President's Commission on Aviation Security and Terrorism have been carried out and the reasons for any delay in carrying out those recommendations			No	1990 Report recommendations fully integrated into subsequent laws, such as Aviation and Transportation Security Act and Homeland Security Act
(7) summary of activities of the Assistant Administrator for Intelligence and Analysis;			No	Included in NSTS Section II Sector Risk Profile. Also developed in TSSRA
(8) financial and staffing requirements of the Assistant Administrator for Intelligence and Analysis;			No	Per citation in previous reports included in budgetary and other required DHS submissions
(9) assessment of financial and staffing requirements, and attainment of existing staffing			No	

Requirement	Year	Due	Included in this Report	Notes
goals, for carrying out duties and powers of the Administrator of TSA related to security; and,				
(10) legislative and regulatory recommendations.			No	Included in DHS annual Congressional data call process
Annual Update on Enhanced Security Measures: Section 109(b), Aviation and Transportation Security Act (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296	November 19, 2001 - PL 107-71 Aviation and Transportation Security Act	19-May[25]	No	All measures closed out
Annual Report on the National Strategy for Public Transportation Security: 6 U.S.C. § 1141	August 3, 2007 - PL 110-53 9/11 Commission Act	31-Mar	Yes	Included as Appendix D

[25] "No later than 6 months after the date of enactment of this Act (Nov 19, 2001), and annually thereafter…"

Appendix D: Public Transportation Security Annual Report 6 U.S.C. § 1141

This appendix addresses the annual reporting requirements of 6 U.S.C. § 1141, covering the implementation of the National Strategy for Public Transportation Security, as defined by Title 6-Domestic Security, Chapter 4-Transportation Security, Subchapter III-Public Transportation Security, Sections 1131 through 1139.

1) Description of the implementation of the provisions of Title XVI of the 9/11 Act (title)

§1131 Definitions

Status: No action required

§1132. Findings

Status: No action required

§1133. National Strategy for Public Transportation Security

Status: Implemented through the 2016 National Strategy for Transportation Security, Appendix D, Surface Security Strategies and Plan.

§1134. Security assessments and plans

Status: See 4)a) and 4)c) below.

§1135. Public transportation security assistance

Status: See 2) below

§1136. Security exercises

Status: TSA published an Advance Notice of Proposed Rulemaking on Surface Transportation Vulnerability Assessments and Security Plans. See 81 FR 91401 (Dec. 16, 2016)

§1137. Public transportation security training program

Status: TSA published a Notice of Proposed Rulemaking on Security Training for Surface Transportation Employees. See 81 FR 91336 (Dec. 16, 2016).

§1138. Public transportation research and development

Status: To ensure market technology maturation, TSA plans, develops, and executes assessment processes to determine innovative and emerging technology suitability, effectiveness, and feasibility in surface transportation venues. This includes laboratory-based evaluations and field assessments in areas such as anomaly explosive detection, intrusion detection, standoff detection, remote screening, and blast mitigation. TSA also coordinates Chemical-Biological and other Weapons of Mass Destruction technology-related activities with DHS Science and Technology and other Federal departments and agencies. TSA coordinates and manages mass transit test beds with non-aviation stakeholders and technology end-users to assess promising technology solutions and other tools to drive mission success, to address current and emerging threats, close capability gaps, and reduce risk of serious disruptions to surface transportation stakeholders. The data gathered from these test beds and the technologies used within them are a major factor in driving priorities in coordination with end-users. TSA collects and analyzes operational needs, technology requirements, and security concerns in collaboration with industry through the formally chartered R&D Working Group and in partnership with DHS Science and Technology. This group serves as the primary mechanism for gathering R&D input, which comes from transportation stakeholders such as DOT, DHS Science and Technology, the Department of Defense, and state and local representatives. TSA also establishes Integrated Project Teams, such as for Standoff Detection, to facilitate increased formal collaboration between key government organizations to enhance and mature standoff detection technologies.

Examples of large-scale projects include:

- Mass Transit Testbeds: Amtrak, Los Angeles Metro, New Jersey Transit, Bay Area Transit, and Washington Metropolitan Area Transit Authority
- Freight Rail Test Beds: Tennessee River Bridge, Plattsmouth Bridge, Hwy 1&9, and Northern Branch Rail Corridor
- Pipeline Test Beds: Compton Roads, Yorktown Junction, and a representative test fixture at the Johns Hopkins Applied Physics Laboratory

Examples of small-scale projects include:

- Special Studies: Blast Mitigation and Bus Studies
- Representative National Special Security Events Support

§1139. Information sharing

Status: The PT-ISAC has provided the government and the commercial transportation industry with alerts, bulletins, information, and analysis concerning terrorist movements, operations, threats and, on rare occasions, reports on suspicious sightings of possible terrorist activity. In turn, such information is jointly shared with TSA and an international association of over 1,500 public and private member organizations and stakeholders. The PT-ISAC functions as a sector-specific platform, providing critical information/intelligence requirements covering threats, incidents, and vulnerabilities facing the transportation sector.

2) Amount of funds appropriated to carry out the provisions of this title that have not been expended or obligated.

The TSGP is one of the Federal Emergency Management Agency's (FEMA) annual grant programs that directly support transportation infrastructure security activities. Section 1406 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53) (6 U.S.C. § 1135), under the *DHS Appropriations Act*, 2016 (Pub. L. No. 114-113), provides the appropriation authority and funds are issued by FEMA. The Table below shows historic TSGP funding levels through FY 2016. TSGP funding has been fully obligated to high-risk public transportation systems; not all funds have been expended as the period of performance for the FY 2015 and FY 2016 grants are still open.[26]

TSGP Totals:

2008-2016	$1.7B[27]	TSGP total public transportation security-related projects funds
2008-2016	$19M	TSGP funds awarded for security planning initiatives
2015-2016	300%[28]	Percentage of TSGP project requests above available funding

The 2016 Enacted Surface Appropriation funding appropriated to TSA for surface transportation-related security activities is reflected in the table below:

2016 Surface Appropriation:

$28.1M	Surface Transportation Security Operations and Staffing
$82.7M	Surface Transportation Security Inspectors
$110.8M	Total appropriation

3) Estimated cost to implement the National Strategy for Public Transportation Security that breaks out the aggregated cost of needed capital and operational security improvements for fiscal years 2008-2018.

The estimated aggregated cost of needed capital and operational security improvements was $6.4 billion for 2015, which is the last projected year in the American Public Transportation Association, Survey of United States Transit System Security Needs, Summary of Findings, dated April 2010[29]. According to the survey, the five-year security-related investment need estimate through 2015 included $4.4 billion for transit security-related capital investment, plus $2 billion for operational security improvements for 35 of its transit agency members, operating 43 percent of all transit vehicles that report in the Federal Transit Administration, National Transit Database and are TSGP eligible. The 2017 estimated adjusted cost to implement the NSTS for the entire high-risk public transportation agency population exceeds $4.7 billion.

4) State of public transportation security in the U.S., including:

a) The status of security assessments;

[26] TSGP period of performance for expenditure of FY 2015 funding is September 2018; for FY 2016 funding it is September 2019.

[27] Federal Emergency Management Agency, Transit Security Grant Program. https://www.fema.gov/transit-security-grant-program

[28] $251 million/309 percent in FY 2015; $293 million/336 percent in FY 2016

[29] American Public Transit Association, Survey of United States Transit Systems Security Needs, Summary of Findings, April 2010. http://www.apta.com/gap/legissues/other/Documents/APTA%20Security%20Survey_April2010.pdf

The voluntary BASE program was used to review security assessments conducted by public transportation agencies. Two-hundred seventeen BASE reviews were conducted from FY 2014 through FY 2016, including 50 on agencies that are in the high-risk category (defined by having an average weekday ridership of more than 60,000 passengers). All high-risk agencies (100 percent) had performed a security assessment of their systems.

b) Progress being made developing prioritized lists of security improvements to secure public transportation facilities and passengers;

TSA and FEMA developed funding priorities for the TSGP and have reviewed those priorities, adjusting as necessary, each year. Agencies submitting applications that align with the funding priorities have a higher probability of receiving an award than proposals that are not aligned. The prioritized funding has resulted in security improvements as projects are completed.

c) Progress made by agencies developing security plans and how those plans differ from the security assessments;

The BASE program assesses public transportation agencies against multiple security-related categories identified by the public transportation community as fundamental for a sound security program, including the presence and quality of a security plan and assessment. The results of the BASE assessments indicate gaps or shortfalls in existing plans and allow the agencies to adjust and strengthen their plans to close the gaps. There was a three percent increase over six years in high-risk agencies having security plans.

d) A prioritized list of security improvements being compiled by other agencies;

TSA and FEMA convened an industry working group of transit agency and security stakeholders to reevaluate the security and funding priorities for the TSGP. The working group developed a list of priority areas and project types it feels reflect the security needs, and are the best ways to address the current threat environment. These changes were implemented for the FY 2016 TSGP application cycle.

The security priorities are:

1. Operational Activities, including training, drills and exercises, public awareness campaigns, and security planning and assessments
2. Operational Deterrence, including K-9 teams, Mobile Explosives Detection Screening Teams, Anti-Terrorism Teams, and surge/directed patrols on overtime
3. Capital Projects, including all types of critical infrastructure remediation, including cyber security

5) A random sample of an equal number of large- and small-scale projects currently underway.

Ongoing projects vary greatly both in type and size. Projects range from lower-dollar amount training, exercise and public awareness projects, to operational deterrence projects to multi-million-dollar infrastructure capital protection projects for stations, bridges, and tunnels.

Examples of large-scale projects currently underway include:

- Securing underground/underwater vulnerable points of entry at TTAL assets
- Perimeter Security at a large, multi-modal TTAL asset
- Physical barriers and electronic security measures at a bridge critical to mass transit operations
- Portable barrier systems at TTAL assets

Examples of small-scale projects currently underway include:

- Sustainment of K-9 teams, mobile screening teams, anti-terrorism teams, and directed/surge patrols on overtime
- "If You See Something, Say Something™" campaign, which was originally created with TSGP funds, and other public awareness campaign materials and resources
- Closed-circuit television and access control at transit stations and platforms

~~FOR OFFICIAL USE ONLY~~

2018 Annual Report On Transportation Security

Calendar Year 2017 Report to Congress

December 6, 2018

Homeland Security

Transportation Security Administration

~~FOR OFFICIAL USE ONLY~~

~~**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

Message from the Administrator

December 6, 2018

I am pleased to transmit the 2018 Annual Report on Transportation Security. This report combines multiple annual reporting requirements to streamline and improve the U.S. Department of Homeland Security's processing and submission of the various annual reports on transportation security.[1] Unless otherwise noted, the report summarizes the activities taken in calendar year 2017 by transportation systems owners and operators, and by federal, state, local, tribal, and territorial government partners to enhance systems protection and resilience for all types of hazards.

To accomplish our security mission, the Transportation Security Administration (TSA) worked collaboratively with a wide range of partners, from Federal agencies, aviation and surface transportation industry stakeholders, and international counterparts to intelligence and law enforcement community professionals. We worked particularly closely throughout the year with our Co-Sector-Specific Agencies for the Transportation Systems Sector, the U.S. Department of Transportation, and the U.S. Coast Guard.

This report satisfies the reporting requirements for the following:

- Annual Periodic Progress Report on the National Strategy for Transportation Security;[2]
- Annual Report on Transportation Security;[3]
- Annual Update on Enhanced Security Measures;[4]
- Annual Report on the National Strategy for Public Transportation Security;[5] and
- Annual Report on the National Strategy for Railroad Transportation Security.[6]

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

The Honorable A. Mitch McConnell, Jr.
Senate Majority Leader

[1] Detailed in a TSA letter to Congress, dated August 11, 2010

[2] 49 U.S.C. § 114(s)(4)(C).

[3] 49 U.S.C. § 44938(a).

[4] Section 109(b) of the *Aviation and Transportation Security Act* (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296.

[5] 6 U.S.C. § 1141.

[6] 6 U.S.C. § 1161.

The Honorable Charles E. Schumer
Senate Minority Leader

The Honorable Kevin McCarthy
House Majority Leader

The Honorable Nancy P.D. Pelosi
House Minority Leader

The Honorable John Thune
Chairman, Committee on Commerce, Science, and Transportation

The Honorable Bill Nelson
Ranking Member, Committee on Commerce, Science, and Transportation

The Honorable Ron Johnson
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Claire C. McCaskill
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Michael D. Crapo
Chairman, Committee on Banking, Housing, and Urban Affairs

The Honorable Sherrod Brown
Ranking Member, Committee on Banking, Housing, and Urban Affairs

The Honorable Michael T. McCaul
Chairman, Committee on Homeland Security

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

The Honorable William Shuster
Chairman, Committee on Transportation and Infrastructure

The Honorable Peter A. DeFazio
Ranking Member, Committee on Transportation and Infrastructure

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

Sincerely yours,

David P Pekoske

David P. Pekoske
Administrator

Executive Summary

The 2018 Annual Report on Transportation Security fulfills multiple annual reporting requirements and summarizes activities that took place in calendar year 2017 (unless otherwise noted) by transportation systems owners and operators, and by federal, state, local, tribal, and territorial government partners to enhance system protection and resilience from terrorism. The report addresses modal-specific actions, as well as cross-sector and intermodal issues related to the management of risks in the Nation's transportation systems, both domestically and internationally.

The table below identifies the Transportation Systems Sector's three security goals, as stated in the 2016 National Strategy for Transportation Security, to achieve a secure and resilient transportation system. The report assesses the sector's progress toward achieving these goals and discusses key accomplishments.

Table 1: Sector Goals

Goal 1:	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Goal 2:	**Enhance effective domain awareness of transportation systems and threats**
Goal 3:	**Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce**

The Transportation Systems Sector continued to build and maintain relationships with state and local officials, owners and operators, international organizations, and U.S. Government partners to share threat information and best practices, enhance domestic and international transportation security, and coordinate U.S. position on a multitude of security issues and mitigation measures. The Transportation Systems Sector's ability to assess security gaps, combined with practically applied risk mitigating activities, leads to continuous improvement of all activities associated with measureable threat detection, deterrence, and resilience goals, and forms the foundation of risk-based security.

Aviation: In 2017, the Aviation Transportation Subsector screened over 750 million commercial aviation passengers (more than 2 million per day).[7] In addition, TSA officers screen over 4.9 million carry-on items and 1.3 million checked items every day.[8]

[7] TSA by the Numbers Fact Sheet https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet_0.pdf

[8] Ibid

At domestic airports, TSA officers conducted random and unpredictable security activities, such as screening of employees, searches of vehicles approaching controlled areas, and canine sweeps. TSA introduced new enhanced carry-on bag procedures for domestic flights that help our officers identify potential threats more effectively. To help mitigate the insider threat, TSA implemented the capability for the Federal Bureau of Investigation's Rap Back Service to provide near real-time notification to TSA of new, potentially disqualifying criminal events that enables airport and aircraft operators to revoke an individual's unescorted access in a responsive manner. In the area of inspections, TSA is working collaboratively with industry to focus on the use of best practices to achieve and sustain the highest compliance and security outcomes.

Internationally, TSA worked to influence key decision makers in foreign locations and industry partners to understand the threat, maintain awareness of vulnerabilities, and encourage operators to implement mitigation strategies. TSA is raising the baseline of global aviation security by assessing compliance with security measures at last point of departure airports and continuing to work with carriers and foreign partners to enhance security procedures and posture.

For public spaces at airports and throughout the transportation system, TSA published the Public Area Security Summit National Framework, which provides a set of recommendations jointly developed with industry, government, academic, international, and public officials to enhance security in open spaces at airports and throughout the transportation system.

Maritime: The Maritime Transportation Subsector, led by the U.S. Coast Guard, developed tools, portals, and capabilities to more effectively share critical information. The U.S. Coast Guard continues to work with security partners and stakeholders to pursue a risk-based security posture. Using the Area Maritime Security Training and Exercise Program, Federal Maritime Security Coordinators and their Area Maritime Security Committees test the effectiveness of their respective port-level Area Maritime Security Plans and support maritime security preparedness regimes through the engagement of federal, state, local, tribal, and territorial government and private sector stakeholders. The U.S. Coast Guard also continued its collaborative work with the National Institute of Standards and Technology to finalize Cybersecurity Framework Profiles for Offshore and Passenger Vessel Operations.

Surface: The Surface Transportation Subsector's primary security focus is on cooperation, coordination, and oversight. Of highlight, TSA conducted over 200 voluntary security assessments for pipeline, mass transit, and over-the-road bus entities and school bus districts and worked with the operators on mitigation approaches that help raise the national security baseline. These review programs analyze security standards and security programs for each system and identify opportunities to further enhance security. TSA facilitated approximately 14 Intermodal Security Training and Exercise Program exercises, half of which involved multiple modes of transportation, to help operators test and evaluate their security plans, including prevention and preparedness capabilities, response abilities, and cooperation with first responders.

The entire Transportation System Sector continues to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints.

2018 Annual Report on Transportation Security

Table of Contents

I. Legislative Language

The 2017 Annual Report on Transportation Security fulfills four annual reporting requirements, including implementation of the National Strategy for Transportation Security (NSTS) and other statutory requirements, as detailed in Appendix B, to achieve efficiency and deliver a coordinated message to the President and Congress. See Appendix B for a full description of the statutory reporting requirements.

II. Sector Description, Vision, and Mission

The Transportation Systems Sector consists of a network of interdependent systems across three subsectors—aviation, surface, and maritime. The Nation's critical infrastructure depends on the transportation systems sector, and in turn, the transportation systems depend on other sectors, such as energy, communications, information technology, chemical, and manufacturing.

The interdependencies are an important dimension of the risk environment that must be considered to protect transportation critical infrastructure and achieve system resilience. A primary focus of the sector's risk management processes during this reporting period was to identify, assess, prioritize, and manage risks in order to enhance the resilience of the transportation systems.

This report describes how the transportation system managed risk and increased resilience based on the goals and objectives stated in the 2016 NSTS. It describes progress in addressing terrorism risks, enhancing resilience, improving domain awareness, and protecting privacy, civil rights, and freedom of movement.

III. Sector Progress

In fiscal year (FY) 2017, there were nine strategic performance measures used to assess TSA's efforts. Sixty-seven percent of the measures met their target and 75 percent maintained or improved actual results compared to FY 2016.

In summary:

- TSA continued to vet 100 percent of domestic passengers and checked baggage each day in order to ensure the safety and security of the travelling public.
- Trusted Traveler programs enrolled more than 3 million more travelers to receive expedited screening, enabling TSA to focus on unknown and high-risk travelers, and TSA achieved more than 5 million travelers enrolled in *TSA Pre✓®*.

- Security partnerships were also effectively strengthened and expanded through United Nations Security Council Resolution 2309 -- Aviation Security, which calls on member states to implement effective, risk-based measures that mitigate the ever-evolving threat picture.
- Within the Intelligence Community, Priority Intelligence Requirements were developed regarding intelligence collection and reporting, and the creation of the Aviation Domain Intelligence Integration and Analysis Cell that enables the government to share information more effectively with the travel industry.
- Compliance with aviation security standards was also strengthened through the completion of international airport assessments and air carrier inspections.
- In Surface transportation, TSA collaborated closely with industry and government partners to identify and secure critical surface transportation assets through technical assistance, training, and exercises.

Table 2: External Performance Results and Plan

Prior Results					2017		Performance Plan	
2012	2013	2014	2015	2016	Target	Result	2018	2019
Percent of air carriers operating from domestic airports in compliance with leading security indicators								
98.1%	98%	98%	98%	98%	100%	97.7%[9]	100%	100%
Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas								
---	---	---	---	---	*New Measure*		95%	95%
Percent of domestic cargo audits that meet screening standards								
---	---	---	---	98%	96%	97.7%	97%	98%
Percent of foreign airports that serve as last points of departure and air carriers involved in international operations to the United States advised of necessary actions to mitigate identified vulnerabilities in order to ensure compliance with critical security measures								
---	100%	100%	100%	100%	100%	100%	*Retired*	
Percent of foreign last point of departure airports that take action to address identified vulnerabilities								
---	---	---	---	---	*New Measure*		70%	70%
Percent of international cargo audits that meet screening standards								
---	---	---	---	97%	96%	97.6%	97%	98%
Percent of overall compliance of domestic airports with established aviation security indicators								
95%	94.4%	94%	95%	93%	100%	93.9%[10]	100%	100%

[9] The percentage of air carriers found to comply with transportation security regulations through inspections. TSA aggressively works with air carriers to ensure they comply with all security requirements and take enforcement and other actions when necessary. TSA will work with air carriers on security deficiencies and vulnerabilities to ensure airports are 100 percent in compliance with the security rules and regulations they follow.

[10] The percentage of airports found to comply with transportation security regulations through inspections. TSA aggressively works with the airports to ensure they comply with all security requirements and take enforcement and other actions when necessary. TSA will work with airports on security deficiencies and vulnerabilities to ensure airports are 100 percent in compliance with the security rules and regulations that they follow.

Percent of overall level of implementation of industry agreed upon Security and Emergency Management action items by mass transit and passenger rail agencies								
39%	69%	78%	80%	71%	75%	73.6%[11]	77%	79%
Percent of passenger data submissions that successfully undergo Secure Flight watch list matching								
---	---	---	---	---	100%	100%	100%	100%
Percent of TSA regulated entities inspected per fiscal year by transportation security inspectors								
---	---	---	---	---	*New Measure*		90%	90%
Average number of days for DHS Traveler Redress Inquiry Program redress requests to be closed								
93	52	62	50	44	< 55	50	< 55	< 55

IV. Modal Progress

The NSTS defines goals and supporting objectives and activities for each subsector and mode of transportation. This section assesses progress toward achieving these goals by providing an assessment of each goal and discussing key accomplishments in the goal's supporting objectives and activities. The transportation security community continues to enhance security through policy, programs, initiatives, and activities developed in collaboration with government and industry partners. These efforts reduce risk associated with potential terrorist attacks in part by increasing system resilience.

A. Aviation Transportation Subsector

The Aviation Transportation Subsector consists of commercial aviation, commercial airports, general aviation, and air cargo. The owners and operators, state and local authorities, and the Federal Government work collaboratively to develop measurable security activities, plans, and objectives needed to achieve threat deterrence, detection, and resilience goals.

In 2017, TSA screened more than 2 million domestic and international commercial aviation passengers daily, averaging over 750 million passengers. Each day, TSA screens 4.9 million carry-on items and 1.3 million checked items for explosives and other prohibited items.[12] The capabilities of airports to process millions of passengers and tens of thousands of tons of cargo every day depend on an estimated 1.8 million workers, most of whom undergo a security threat

[11] As of September 30, 2017, 39 of 53 Mass Transit Systems met the criteria as measured by Baseline Assessment for Security Enhancement (BASE) assessments, just shy of the target of 75 percent. Efforts to improve BASE scores will focus on information sharing activities to include emphasizing implementation of modal security action item best practices in those areas with low scores. TSA will provide information and recommendations for improvement, in particular highlighting the availability of TSA training and exercise resources. Transit agencies will also be encouraged to review practices in place at counterpart agencies with superior programs.

[12] https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet_0.pdf

assessment to have access to secured areas and other Security Identification Display Areas, Sterile Areas, and/or to Air Operations Areas at U.S. airports. For the past several years, the Federal Aviation Administration (FAA)/TSA Airspace Waiver Program has issued approximately 6,000 international waivers annually to foreign private charter and general aviation aircraft operating in U.S. airspace.

Table 3: Aviation Progress Assessment

Goal 1: Manage risks to aviation transportation systems from terrorist attacks and enhance system resilience
Overall Assessment: TSA continued to build and maintain relationships with government officials, owners and operators, civil authorities, international organizations, and U.S. Government partners to share threat information and best practices, enhance domestic and international transportation security, and coordinate the U.S. position on a multitude of security issues and mitigation measures. At domestic airports, TSA conducted random security activities, such as searches of vehicles approaching controlled areas of airports and canine sweeps. Internationally, TSA worked to influence key decision makers in foreign locations and industry partners to understand the threat, maintain awareness of vulnerabilities, and encourage operators to implement mitigation strategies. TSA continued to enhance air domain awareness with security partners and stakeholders at open-forum meetings of aviation security stakeholders.
Objective 1: Improve physical and cyber security of domestic aviation critical infrastructure
Activity 1: Increase frequency of recurrent criminal history records checks for credentialed airport workers with unescorted access to secure airport areas. **Key Accomplishment:** Implemented the Federal Bureau of Investigation's (FBI) Rap Back Service to provide near real-time notification of new, potentially disqualifying criminal events that enables TSA, and airport and aircraft operators to revoke an individual's unescorted access, substantially mitigating the insider threat posed by individuals with disqualifying offenses. In 2017, 65 airports enrolled with the service and an additional 65 have executed a memorandum of understanding with TSA to enable future participation.[13]

[13] The Rap Back Service is a subscription service offered by the FBI whereby the subscriber is provided with continuous updates to the criminal history of its covered workers. TSA facilitates the establishment and management of Rap Back subscriptions for airports that chose to enroll their SIDA badge holders in Rap Back, and TSA also acts as a conduit from the FBI to the airport for the resulting criminal history updates for affected SIDA badge holders.

Activity 2: Conduct outreach with aviation security partners on the voluntary implementation of the principles and best practices of risk management through the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

Key Accomplishments:

- Conducted a cybersecurity awareness webinar for 300 participants to familiarize sector stakeholders with the Federal cyber risk management support available to critical infrastructure owners and operators. The webinar included a promotion to adopt the NIST Cybersecurity Framework and encourage the use of the Transportation Systems Sector Framework Implementation Guidance.
- Conducted five regional cybersecurity workshops for stakeholders, which included airport authorities, with the primary objective of raising awareness of available risk management support products, and providing an opportunity for stakeholders to exchange best practices and lessons learned.
- Facilitated a one-day cybersecurity tabletop exercise and strategy session to identify cybersecurity challenges, gaps, and successes across the sector. Participants included airline, airport, and trade association representatives.

Activity 3: Focus security resources on higher-risk travelers, workers, facilities, aircraft, cargo, and baggage.

Key Accomplishments:

- The Enhanced Accessible Personal Property initiative began rollout of enhanced screening procedures for carry-on baggage, which was fully implemented in 2018. These procedures require travelers to place all personal electronics larger than a cell phone in bins for X-ray screening in standard lanes, as part of a greater effort to raise the baseline for aviation security.
- Employed a risk-based strategy through testing airport and airline compliance to reduce the threat to aviation security within the areas with the highest aviation worker activity to reduce the insider threat.
- Continued to use the Visible Intermodal Prevention and Response (VIPR) Program's risk-based Concept of Operations to focus VIPR deployments at aviation facilities with the greatest degree of risk.
- Strategically focused law enforcement resources to mitigate high-risk travelers aboard U.S. flagged commercial flights.
- Participated in the White House initiative to revise and update the National Strategy for Aviation Security.

Objective 2: Improve preparedness and response capabilities to deter, detect, respond, and recover from terrorist attacks throughout the aviation community

Activity 1: Improve training for frontline employees to identify, deter, prevent, and respond to threats to the homeland.

Key Accomplishments:

- Through the TSA training centers at Glynco, GA and Atlantic City, NJ, trained 12,677 students, and offered coursework in 52 separate security and management subjects.
- Continued centralizing the training of newly hired Transportation Security Officers (TSOs) at the TSA Academy at the Federal Law Enforcement Training Center. To support this initiative, TSA completed an $11 million project and established a state-of-the-art learning center at the TSA Academy.
- TSA's Canine Training Center (CTC) executed a 17 percent year-over-year increase in canine team production through a self-initiated efficiency analysis that reduced initial training course length. As a result, the CTC trained 300 canine teams, more teams than any other comparable time period.
- Launched the first mandatory training programs for J-K-Band employees through the TSA Leadership Institute's School of Senior Leadership Studies. TSA also designed and facilitated the first TSA Senior Executive Service training and development program.
- Designed, developed, and launched the first training course for TSA's newly hired employees in the Management, Administrative, and Professional (MAP) job categories. With this week-long program, TSA is able, for the first time, to instruct its MAP new hires about the Agency's mission and core values, and introduce them to field operations at the Philadelphia International Airport and Federal Air Marshal Service training sites.

Activity 2: Execute and enhance vetting of passengers and aviation credentialed holders, as well as indications and warning of potential threats to aviation sector.

Key Accomplishments:

- Used Secure Flight Passenger Data to strategically deploy Federal Air Marshal teams on basis of risk aboard U.S. flagged commercial flights to mitigate potential threats.
- Continued TSA's Insider Threat Program outreach to domestic stakeholders to support development of similar programs across all of the nation's commercial airports.
- Expanded internal partnerships to provide Insider Threat Awareness training for aviation sector personnel, emphasized through training and awareness campaigns, such as *See Something, Say Something™* and *This is My Airport.*

Objective 3: Enhance international aviation security risk management strategies

Activity 1: Conduct outreach to facilitate the use of international best practices and procedures.

Key Accomplishments:

- Enhanced in-flight security efforts by hosting an Inflight Security Officers Conference attended by officers from seven nations.
- Reduced international aviation risk by implementing a Federal Air Marshal Service International Concept of Operations.
- Continued TSA's Insider Threat Program outreach to international stakeholders to support development of similar programs across all of the international last points of departure for commercial flights into the United States.

- Enhanced security effectiveness and mitigated risks to global aviation by evaluating and documenting security at foreign airports with service to U.S., airports from which U.S. air carriers operate, and other sites on a 5-point scale against critical International Civil Aviation Organization (ICAO) aviation and airport security standards. TSA assessed compliance with these standards and provides feedback to the host governments for awareness and recommended follow-up action.
- Developed international threat analysis requirements to support enhanced risk analysis incorporated into the Transportation Sector Security Risk Assessment (TSSRA), the Cities and Airports Threat Assessment (CATA), and the Foreign Airport Threat Assessment (FATA).

Activity 2: Assess compliance with security measures for international inbound passengers, cargo, and baggage.

Key Accomplishments:

- Conducted 143 foreign airport assessments; 2,175 air carrier inspections; 28 capacity development training activities; and vetted 557 aviation security personnel from 29 countries.
- Issued Security Directives (SDs) and Emergency Amendments (EAs) to be implemented by air carriers at select locations when specific threats are identified or significant vulnerabilities warrant additional mitigation actions. TSA used a number of methods, such as ad hoc visits or inspections to verify compliance with the additional measures. TSA coordinated the issuance of 56 SDs/EAs for non-U.S. locations.

Objective 4: Increase security technology capability to respond to known and emerging threats

Activity 1: Improve industry participation in the Research and Development (R&D) process for threat detection and screening capabilities.

Key Accomplishments:

- Completed the Innovation Task Force's (ITF) second Broad Agency Announcement, receiving 96 solution submissions and selecting 12 for future demonstration. The ITF currently has 11 "Innovation Sites" with three more applications under review.
- The ITF developed a robust industry exchange strategy to creatively engage with industry, promote partnerships, and accelerate innovation across the transportation security ecosystem. In June 2017, the ITF hosted an Industry Day, promoting international engagement and collaboration as a primary method to achieve success by identifying approaches, methodologies, and solutions to enhance U.S. aviation security. The ITF was able to engage with 96 unique solution providers, 42 of which had not previously interacted with TSA, resulting in a 14 percent increase from the previous Industry Day
- The ITF demonstrated five distinct solution technologies in partnership with stakeholders across the transportation ecosystem including: 1) Automated Screening Lanes, 2) Computed Tomography X-Ray, 3) Biometric Authentication Technology, 4) Checkpoint Planning and Staffing Allocation, and 5) Colorimetric Explosives Trace

Detection (ETD). In addition, the ITF participated in two ITF-enabled solutions:[14] 1) Biometric Bag Drop and 2) Large Mass Threat Detection.

Activity 2: Improve aviation safety and security capabilities to detect illegal use of unmanned aircraft systems.

Key Accomplishment: Vetted approximately 75,000 Unmanned Aircraft Operator Certificates daily, as required under 14 C.F.R. part 107. TSA continues to engage with FAA and other security partners (DHS, U.S. Department of Defense, & U.S. Department of Justice), U.S. Customs and Border Protection (CBP), and various others to ensure the safe and secure integration of unmanned aircraft systems into the National Airspace System.

Goal 2: Enhance effective air domain awareness of transportation systems and threats

<u>Overall Assessment</u>: The Aviation Subsector continued to enhance air domain awareness with security partners and stakeholders in 2017 at open-forum meetings of aviation security stakeholders, such as the Aviation Security Advisory Committee (ASAC), and the Aviation Government Coordinating Council and Sector Coordinating Council. The Aviation Subsector worked with its security partners to assess the security at airports, analyze the aviation security attack scenarios posing the greatest risks, develop mitigation plans to address the highest priority areas, and share intelligence and best practices.

Objective 1: Improve quality and timeliness of intelligence and information products for government, industry and public awareness

Activity 1: Improve public awareness of security issue reporting channels and dissemination of actionable threat information among partners (e.g., *See Something, Say Something* ™, General Aviation Watch, and *This is My Airport* Programs).

Key Accomplishments:

- Developed and provided Insider Threat Awareness training for aviation sector personnel, emphasized through training and awareness campaigns, such as *See Something, Say Something* ™ and *This is Our Airport.*
- Streamlined the process for sharing suspicious incident reporting with local, state, tribal and territorial, and Federal criminal justice agencies through the FBI's National Data Exchange system.
- Implemented the Cities and Airports Threat Assessment system, which ranks over 440 airports based on threat attractiveness. It is updated and published monthly for stakeholders.

Activity 2: Expanded intelligence information sharing with industry through classified and

[14] Enabled projects are demonstrations led by a non-TSA entity looking to identify new and emerging capabilities that are conducted at the entity's local setting in conjunction with the local airport authority. The ITF's role in these projects is to provide coaching through the structured process similar to a successful full-scale demonstration.

unclassified means.

Key Accomplishments:

- Produced and disseminated 43 Country Threat Assessments looking at international threats to U.S. civil aviation and Western interests. Conducted 52 unique in-person engagements consisting of threat briefings to individual airlines and trade associations, and site-visits to industry facilities, providing timely and accurate information to industry partners.
- Produced the 2017 Annual Civil Aviation Threat Assessment and the 2017 Annual Transportation Cyber Threat Assessment, which establish a baseline assessment of threats to U.S. aviation by reviewing terrorist threats to U.S. civil aviation worldwide.
- Conducted the Annual Transportation Sector Security Risk Assessment, which assessed the overall risk to aviation in 2017.
- Deployed approximately 68 Field Intelligence Officers and 14 Liaison Officers who provided direct support to TSA field locations and representation at partner organizations. Field Intelligence Officer staffing increased by 17 to expand coverage and intelligence support. Field Intelligence Officers also delivered more than 5,103 intelligence briefings as part of TSA's overall Mission Essentials - Threat Mitigation training program to increase security effectiveness of the TSA frontline workforce, and delivered 496 intelligence briefings to aviation stakeholders.
- Formalized an unprecedented arrangement with key stakeholders to share aviation security-related information and intelligence through the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC). It is a single aviation domain sharing hub for the dissemination of intelligence and threat-related information to a growing network of industry and agency partners.

Objective 2: Improve collaboration among private sector and government agencies regarding intelligence and information sharing

Activity: Increase discussion of strategic priorities as an agenda item at open-forum meetings of aviation security stakeholders. Examples include Public Area Security Summit and ASAC meetings.

Key Accomplishments:

- Published the Public Area Security Summit National Framework, which is a set of recommendations jointly developed with industry, government, academic, international, and public officials that enhances security in public spaces at airports and throughout the transportation system. The group worked together to leverage a wide network of transportation and security officials to codify a framework that deters terrorist attacks and creates a system that quickly and effectively responds to attacks in the public area to minimize loss of life and disruption of transportation.
- Participated in the Quarterly Airport Security Review with the airport industry, which has led to meaningful collaborative sessions to update current security policy and provide strong joint efforts on new initiatives.

- Continued to implement recommendations provided by the ASAC on aviation workers' access to secure areas.
- Formally established the ADIAC to integrate full-time aviation sector intelligence and information-sharing best practices across the interagency, intelligence community, and aviation private sector at a secure facility.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: The Aviation Subsector continues to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints. The subsector also improved the efficiencies of security measures for passengers by increasing enrollment in expedited screening programs, such as *TSA Pre✓®* application program and other trusted traveler programs. *The TSA Pre✓®* application program reached a milestone in July 2017 of more than 5 million travelers enrolled and now has more than 390 application centers nationwide. TSA's social media customer service program provided timely information, improved customer service, and useful interactions with the American people. This award-winning outreach program is designed to better prepare travelers for security screening, thereby reducing traveler stress and improving the screening process while allowing transportation security officers to focus on the security mission.

Objective 1: Reduce the potential negative impact of security policies and activities to privacy, civil rights, and civil liberties

Activity: Develop policy pursuant to applicable privacy, civil liberties, and civil rights laws and regulations.

Key Accomplishments:

- Performed significant outreach and training to field operations to address transgender passenger complaints regarding screening.
- Continued to grow TSA's social media presence in 2017. TSA's Instagram account has more than 840,000 followers and was one of five nominees for two prestigious Webby Awards next to the likes of Conan O'Brien and The Onion. The main Twitter account shared 1,100 tweets, resulting in more than 31 million impressions and over 206,000 followers. In November, TSA officially launched a Facebook page and broadcasted its first *Ask Me Anything* on Facebook Live with more than 5,000 views.
- Processed 1,698 redress requests with an average response time of 44 days, which improves on the DHS High Priority Performance Goal of less than 60 days.

~~**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

- Published a Privacy Impact Assessment (PIA) for the TSA Contact Center, as a stand alone from the DHS General Contact Lists PIA, and updated the PIA for the Encounters Analysis Program.[15]

Objective 2: Apply risk-based security approach to supply chain and traveler movements

Activity: Enhance efficiency and effectiveness of cargo and traveler screening.

Key Accomplishments:

- Implemented an Outcome Focused Compliance initiative to work collaboratively with industry to use best practices to achieve and sustain the highest compliance and security outcomes. This initiative will enhance collaboration in order to identify problems and solution together.
- Increased *TSA Pre* ✓® application program enrollment by 113 percent to more than 5 million travelers, allowing these prescreened low-risk travelers to experience expedited, more efficient security screening and enhancing the overall efficiency and effectiveness of the screening process.
- Ninety four percent of *TSA Pre* ✓® passengers waited less than 5 minutes.
- Completed over 34,400 cargo-related inspections, which incorporated Special Emphasis Inspections that focused on security vulnerabilities within the cargo supply chain.

[15] Privacy documents for TSA listed at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

B. Maritime Transportation Subsector

The U.S. maritime transportation system is a vital part of the national economy, playing a key role in the global supply chain. It consists of 25,000 miles of navigable channels, 238 locks at 192 locations, and over 3,700 marine terminals at 360 ports. Waterborne cargo and associated activities contribute more than $649 billion annually to the U.S. Gross Domestic Product and sustain more than 13 million American jobs.[16] More than 99 percent of the volume of overseas trade (62 percent by value) enters or leaves the United States by ship.[17] By their nature, waterways are generally less restricted and are freely accessible to transit without many of the mechanisms for detection and investigation often available in the air and land domains. Maritime security vulnerabilities and the potential consequences from a variety of hazards, including hurricanes, terrorist attacks, and cyber threats continue to be significant.

The U.S. Coast Guard (USCG) and its partners maintain a suite of performance measures to monitor progress in meeting *Maritime Transportation Security Act* (MTSA) performance goals and objectives. Refer to the following reports for further information on key maritime security-related performance and metrics:

- DHS Annual Performance Report for Fiscal Years 2016-2018;
- CBP 2017 Border Security Report;
- Threat of Terrorism to U.S. Ports and Vessels Report to Congress, dated August 25, 2017; and
- DHS Fiscal Year 2017 Performance & Accountability Reports.

Table 4: Maritime Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience
<u>2017 Overall Assessment</u>: The Maritime Transportation Subsector (MTS) continues to work with security partners and stakeholders to pursue a risk-based security posture. Using the Area Maritime Security Training and Exercise Program (AMSTEP), Federal Maritime Security Coordinators and their Area Maritime Security Committees (AMSC) test the effectiveness of their respective port-level Area Maritime Security (AMS) Plans and support maritime security preparedness regimes through the engagement of federal, state, local, tribal, and territorial government and private sector stakeholders. The USCG released a draft cyber Navigation and

[16] Maritime Administration, *Marine Transportation System Important Facts*. Available at https://origin-www.marad.dot.gov/ports/marine-transportation-system-mts/ Accessed April 5, 2018.

[17] Ibid.

Vessel Inspection Circular (NVIC) for public comment, which highlights our commitment to open dialogue with the maritime industry to ensure future collective buy-in on managing cyber risks. The USCG also continued its collaborative work with NIST to finalize Cybersecurity Framework Profiles for Offshore and Passenger Vessel Operations.

Objective 1: Utilize risk-based security planning and operations to reduce the terrorism risk to the MTS
Objective 2: Reduce security vulnerabilities and improve preparedness throughout the MTS

Activities:

- Expand cybersecurity protections in all segments of the MTS using the NIST Framework.
- Improve compliance at MTSA facilities through risk-based adjustment of enforcement operations tempo.
- Improve interoperability of Federal, state, local, tribal, and territorial response teams in Maritime Security and Response Operations.
- Employ a Maritime Security Risk Analysis Model and other risk assessment and analysis tools to refine the estimates of maritime security and response operations activities' risk reduction benefits, and use these estimates to inform the execution of Maritime Security and Response Operations activities in U.S. ports.
- Improve International Ship and Port Facility Security Code implementation in foreign ports that send ships to the United States.
- Explore potential use of floating security barriers at critical infrastructure and key resources to provide deterrence and resilience.
- Conduct random, unpredictable operations, such as Visible Intermodal Prevention and Response (VIPR) team deployments, to mitigate terrorist risk to the traveling public and maritime infrastructure.

2017 Key Accomplishments:

- The USCG's International Port Security (IPS) Program conducted assessments of 156 foreign port facilities in 52 countries in 2017 while imposing conditions of entry on vessels arriving from 19 countries. The IPS Program also conducted 32 capacity building activities in 13 countries with marginal port security in order to improve the effectiveness of the countries' anti-terrorism measures in place at their ports. This program coordinates closely with the Department of State in conducting its mission.
- As part of the MTSA security program, Facility Inspectors conducted a combined 58,234 visual and/or electronic inspections of Transportation Worker Identification Credential (TWIC) cards and identified 693 instances of non-compliance with TWIC requirements.
- The USCG released a draft cyber NVIC for public comment, which highlights our commitment to open dialogue with the maritime industry to ensure future collective buy-in on managing cyber risks.

- Completed more than 5,900 security compliance inspections required by the Security and Accountability For Every Port Act of 2006 (SAFE Port Act, Pub.L. 109–347).

Goal 2: Enhance effective domain awareness of maritime transportation systems and threats

<u>2017 Overall Assessment</u>: The Maritime Transportation Subsector developed tools, portals, and capabilities to more effectively share critical information. The USCG continues to work with security partners on enhancing Maritime Domain Awareness tools and capabilities. Specific focus has been to improve the reporting of cyber-related security incidents and modification to the MTS Recovery Common Assessment and Reporting Tool to include new categories of Essential Elements of Information this year. The USCG also retired the legacy Homeport system and implemented Homeport 2.0. The new system's upgrades included fewer site navigation menus and more efficient and secure search functions.

Objective 1: Improve the security, resilience, and regulatory (Federal/state/local/tribal/territorial) information sharing process throughout the MTS community
Objective 2: Improve MTS stakeholder participation in the risk management process for security and resilience prioritization and programming

Activities:

- Enhance Maritime Domain Awareness tools and capabilities.
- Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of data from the Maritime Security Risk Analysis Model.
- Enhance resilience of cyber systems through expanded exercises and assessments.

2017 Key Accomplishments:

- The USCG Homeport Internet Portal (HIP) was used to facilitate compliance with the requirements set forth in the MTSA by providing secure information dissemination, advanced collaboration, electronic submission and approval for vessel and facility security plans, and complex electronic and telecommunication notification capabilities.
- The National Maritime Security Advisory Committee (NMSAC) provided recommendations on the USCG's Guidelines for Addressing Cyber Risks at MTSA-regulated facilities. NMSAC continued its efforts with the Chemical Transportation Advisory Committee to provide recommendations to the USCG on the development of security measures aimed at preventing incidents involving the use of hazardous cargoes as weapons in the maritime environment. Finally, NMSAC members assisted the USCG in making recommendations in its regulatory reform effort, as outlined in Executive Orders 13771 and 13783.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

2017 Overall Assessment: The Maritime Subsector continues to work with its security partners and stakeholders on privacy and the civil rights and liberties of individuals and entities to ensure the freedom of movement.

Objective: Collaborate with international partners to increase the resilience of key foreign ports and foreign infrastructure critical to the MTS and global supply chain

Activities:

- Enhance joint CBP/USCG practices and use of the Maritime Infrastructure Recovery Program for the expeditious recovery of trade after an attack.
- Enhance preparedness of ports through the Area Maritime Security Committee Improvement Process.

2017 Key Accomplishment:

- Using AMSTEP, Federal Maritime Security Coordinators and their AMSC test the effectiveness of their respective port-level AMS Plans and support maritime security preparedness regimes through the engagement of Federal, state, local, tribal, and territorial government, and private sector stakeholders. The following training events were conducted:

Training Events		Seminars	Workshops	Tabletop Exercises	Functional Exercises	Full-scale Exercises	AMS Drills	AMS Games	Maritime security operations*
2016	93	11	4	28	11	21	12	1	5
2017	81	7	8	24	8	12	18	0	4

*Received exercise credit since operations were conducted during real events.

C. Surface Transportation Subsector

The Surface Transportation Subsector enhances security through a risk-based approach to prevent terrorist attacks, protect people and critical assets and systems, and support response to national transportation security incidents. The subsector consists of four transportation modes: Mass Transit and Passenger Rail, Freight Rail, Highway and Motor Carrier, and Pipeline.

The strategy is to identify risk and implement mitigating activities within the stakeholder and security partner areas of security operations. The subsector's ability to analyze gaps identified by a vulnerability assessment process and apply practical mitigating activities leads to continuous improvement of activities associated with the threat detection, deterrence, and resilience goals.

To remain effective in a changing surface transportation threat environment, the Subsector continually engages in research and development by planning, developing, and executing assessment processes to determine innovative and emerging technology suitability, effectiveness, and feasibility in surface transportation venues. It also coordinates and manages test beds with non-aviation stakeholders and technology end-users to assess promising technology solutions and other tools to drive mission success, address current and emerging threats, close capability gaps, and reduce risk of serious disruptions to surface transportation stakeholders. Modal-specific tests beds are discussed in the below tables.

Changes to policy, regulations, legislation, or budget are identified in this annual review where necessary. These assessments highlight issues associated with the NSTS implementation strategies, information sharing and risk analyses that continue to advance progress of NSTS goals, objectives, and activities.

The subsector's primary security focus is on cooperation, coordination, and oversight. Of highlight, TSA conducted over 200 voluntary security assessments for pipeline, mass transit, and over-the-road bus entities and school bus districts to help raise the national security baseline, which is consistent with the level of assessments conducted in past years. These review programs analyze security standards and security programs for each system and identify opportunities to further enhance security.

Table 5: Mass Transit and Passenger Rail (MTPR) Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience
<u>Overall Assessment</u>: In 2017 MTPR security partners continued to pursue a risk-based security posture. TSA and the system owners and operators jointly develop security policies and initiatives to secure MTPR systems, including conducting drills and exercises, promoting security awareness training, identifying and facilitating infrastructure protection, and promoting and conducting operational deterrence activities. Two examples include the Amtrak-led Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE), and the VIPR Program. These activities provide heightened station and right-of-way patrols, increased security presence onboard trains, explosives detection canine sweeps, random passenger bag inspections, and counter-surveillance. Amtrak and partners conducted eight RAILSAFE operations averaging over 150 stations and 1,000 personnel. This program, coupled with more than 2,600 random VIPR deployments, provide an important and robust operational deployment capability for the industry. It is also important to note that many of our partners conduct these activities on a routine basis through their anti-terrorism programs. TSA facilitated seven Intermodal Security Training and Exercise Program (I-STEP) exercises, helping transportation entities test and evaluate their

security plans, including prevention and preparedness capabilities, response abilities, and cooperation with first responders. In addition, the Exercise Information System (EXIS), which is a TSA-sponsored online exercise tool, guides government and industry users through the exercise planning process and provides resources to design, document, and evaluate exercises for all transportation modes. While TSA works with many operators on conducting planning and coordinating exercises, many public transportation agencies conduct routine drills and exercises as part of their overall security program.

Objective 1: Sustain effective security assessments and planning in the critical mass transit and passenger rail industries through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences

Activity: Develop, periodically review, and update security plans based on available information.

Key Accomplishments:

- Conducted over 40 Baseline Assessment for Security Enhancement (BASE) evaluations at high-risk agencies (i.e., those with at least 60,000 daily unlinked passenger trips) to review established written security programs and emergency management plans. Results indicated that 85 percent of the assessed systems received a passing score equal to or greater than 70 percent, indicating that these agencies have effective planning and management processes in place.
- Assessed the vulnerabilities of MTPR vehicles through modeling and simulation, and live explosive validation, in partnership with the U.S. Department of Transportation's (DOT) Transportation Technology Center Inc.

Objective 2: Provide effective security training for frontline employees of mass transit and passenger rail entities

Activity: Conduct training of frontline employees to enable them to identify, prevent, deter, and respond to threats.

Key Accomplishments:

- Trained 143 MTPR individuals on *First Observer Plus* ™.
- BASE evaluations conducted at high-risk agencies to measure progress in establishing and maintaining Security and Emergency Training Programs showed that 85 percent of those systems assessed received a passing score equal to or greater than 70 percent, indicating that agencies continue to excel in maintaining effective security training programs. Public Transportation agencies continue to train their employees, update and modify programs as appropriate, and use federal resources as needed.
- Distributed approximately 41,185 Counterterrorism Guides to 28 transit organizations, the American Public Transportation Association (APTA) members, and 18 TSA Surface Inspector field offices. Provided over 13,465 Cyber Counterterrorism Guides to 20 MTPR organizations and 17 TSA Surface Inspector field offices for expanded distribution to appropriate frontline employees as part of a cooperative effort to

improve MTPR system security.

- Adjudicated comments for the Security Training Surface Transportation Employees Notice of Proposed Rulemaking (NPRM). The Final Rule is on the DHS Unified Agenda to be published in 2018, subject to regulatory reform requirements under Executive Order 13771, Reducing Regulation and Controlling Regulatory Costs.
- Adjudicated comments on the Surface Transportation Vulnerability Assessments and Security Plans (VASP) Advanced Notice of Proposed Rulemaking (ANPRM).

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Mass transit and passenger rail systems either conduct or participate in exercises designed to evaluate the preparedness for, and response to security events.

Key Accomplishments:

- Completed seven I-STEP exercises, which is in line with program targets and goals, at the following locations: Austin, TX; Chicago, IL; Newark/Amtrak, Sonoma, CA; Minneapolis, MN; Los Angeles, CA; and Cleveland, OH.
- Conducted a Chemical Workshop with 11 industry partners, three associations, FBI, DOT, and Federal Emergency Management Agency (FEMA) representatives to enhance preparedness and prevention for the sector.
- Developed the Security Enhancement Through Assessments (SETA) pilot program to simulate a coordinated terrorist attack by covertly placing unattended bags/suspicious bags on multiple transit vehicles simultaneously. Two SETA activities were conducted in 2017. The SETA program consists of five elements that are completed in three phases:
  - Identifying vulnerabilities and establishing the baseline security posture.
  - Mitigating the vulnerability through security training.
  - Reassessing and developing plans to maintain an effective security posture.

Objective 4: Maintain and enhance programs to appropriately secure critical surface transportation physical and cyber infrastructure

Activity: Establish criteria to identify infrastructure that is most critical.

Key Accomplishments:

- Awarded over $17.2 million for assets on the top transit asset list (TTAL) and another $29.2 million for other critical infrastructure protection projects through the Transit Security Grant Program (TSGP) in FY 2017. The TTAL consists of 68 nationally recognized critical infrastructure assets, such as stations, bridges, and underwater tunnels, considered vital to the functionality and continuity of major transit systems, as compiled by TSA in collaboration with industry partners and other federal agencies. Examples of funding priority areas include mobile explosive screening and canine teams, vulnerability assessments and security plans, drills and exercises, and training. Since 2006, more than $991 million has been awarded for TTAL and other critical infrastructure protection remediation projects.

- Worked closely with owners and operators to introduce new technology and approaches to securing public spaces in transportation. TSA invests its resources to help these owners and operators assess risks in their operations and then works with them to develop and implement risk-mitigating solutions. The inherently open and expansive scope of transportation public spaces and the evolving threat require TSA to continue researching and developing innovative processes and technologies to increase security without creating undesired financial or operational burdens. TSA incorporates the needs and capability gaps regarding public spaces into our work to influence and stimulate the development of new security technologies in the marketplace. TSA has established collaborative operational test beds across the country for the MTPR mode, and critical infrastructure protection security technology projects to address the threat demonstrated from attacks worldwide.
- Utilized the test bed program to assess marketplace and emergent technologies to improve MTPR security. Large-scale projects were conducted with Amtrak, Los Angeles Metro; New Jersey Transit; Bay Area Transit; and Washington Metropolitan Area Transit Authority. Examples include next generation at-range standoff person-borne improvised explosive device detection technologies, under-vehicle screening at-speed technologies, and other significant breakthroughs in advanced infrastructure protection.
- Conducted 3,702 Risk Mitigation Activities for Surface Transportation (RMAST) assessments, which use risk-based, intelligence-driven processes and procedures to mitigate current threats and vulnerabilities. During pre-operational planning, TSA, in collaboration with stakeholder security personnel, determines which risk mitigation activities are used, and progress/results are tracked by TSA. RMAST activities were assessed with the SETA program, indicating an overall improvement of 44 percent in 2017, from 32 percent to 76 percent, once RMAST was deployed.

Objective 5: Maintain and enhance programs to appropriately secure the physical and cyber components of critical mass transit and passenger rail infrastructure and systems

Activity: MTPR systems continue to apply measures that mitigate security risks of the transportation network.

Key Accomplishments:

- MTPR stakeholders, transit police, FBI, and cybersecurity experts participated in the annual MTPR Security Roundtable in Baltimore, MD. Industry continues to indicate that this forum provides valuable security information and insights.
- Conducted five cybersecurity workshops across the nation in partnership with industry.
- Continued to work with the MTPR community to provide data and information gleaned from five MTPR technology test beds across the country.

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: Collaboration between TSA and industry on intelligence and information products, best practices, and protective measures occurs through daily interaction and engagement, as well as through formal structures, including the DHS-led Critical Infrastructure Partnership Advisory Council framework, Sector Coordinating Council, and other industry-centric organizations, such as the Mass Transit Policing and Security Peer Advisory Group that represents the top high-risk MTPR systems across the United States, Canada, and the United Kingdom. TSA also strongly encourages the use of the *See Something, Say Something* ™ public awareness campaign. Similarly, TSA's *Not On Our Watch* program is focused on the surface transportation community and is designed to make employees of surface transportation systems part of awareness programs intended to safeguard transportation systems against terrorism and other threats.

Objective 1: Maintain and enhance the means and mechanisms for receiving suspicious information reports from transit agencies, passenger rail operators, and personnel, and for sharing timely and relevant information and intelligence between government agencies, and mass transit and passenger rail operators

Activity: Evaluate and improve the quality of intelligence and information products and the unclassified information delivery system provided to the mass transit and passenger rail owners and operators.

Key Accomplishments:

- MTPR operators reported significant security concerns to the Transportation Security Operations Center, which then provides daily, monthly, and annual reports with analysis of trends.[18] The monthly and annual reports are forwarded to MTPR security coordinators.
- MTPR stakeholders, transit police, FBI, and cybersecurity experts participated in the annual MTPR Security Roundtable. Physical and cybersecurity experts came together to inform and share their perspective on law enforcement and cybersecurity issues.
- APTA convened a Communications and Control Systems Recommended Practice Working Group meeting with industry and the DHS National Cybersecurity Communications and Integration Center (Industrial Control Systems-Cyber Emergency Response Teams) to review and discuss DHS incident response support capabilities for the Nation's top passenger rail agencies.

Objective 2: Engage first responders and the public to understand community risks related to mass transit passenger rail infrastructure and services, to promote preparedness for security concerns, and to improve community resilience

[18] Required by 49 C.F.R. 1580.203

Activity: Promote use of effective public awareness campaigns in communities served by mass transit and passenger rail operations.

Key Accomplishments:

- Facilitated over 12 Peer Advisory Group and industry-wide calls, scheduled monthly or event-driven, to discuss emerging threats, intelligence updates, security challenges overseas, and issues of national MTPR security concern.
- Hosted monthly transit industry information sharing teleconference calls to disseminate intelligence information and security program updates.
- Issued two Surface Transportation Cybersecurity Awareness Messages and 14 Security Awareness Messages (SAM) during times of heightened alert or in response to terrorism events, providing security information and awareness information that emphasize threat-specific existing security measures and/or recommend voluntary protective measures.
- Supported eight Amtrak-led Operation RAILSAFE activities that were planned for the year. On average, RAILSAFE activities included over 170 agencies across 41 states, over 1,000 personnel, and over 150 stations per event.
- Funded APTA to manage the Public Transportation Information Sharing and Analysis Center (PT-ISAC) that provides a 24/7 Security Operating Capability for MTPR-specific critical information/intelligence requirements for incidents, threats, and vulnerabilities. It also disseminates the Transit and Rail Intelligence Awareness Daily Report and offers additional cyber daily reports, as well as other critical reports.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

Overall Assessment: The MTPR mode continued to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints. TSA's social media customer service program provided timely information, improved customer service, and useful interactions with the American people. This award-winning outreach program is designed to better inform travelers of security initiatives, thereby reducing their stress and improving the security process.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy pursuant to applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishments:

- Evaluated all field activities to ascertain compliance with established laws, regulations, and policy.

- Performed significant outreach and training to educate field operations on transgender issues.
- Published a Privacy Impact Assessment (PIA) for the TSA Contact Center, as a standalone from the DHS General Contact Lists PIA, and updated the PIA for the Encounters Analysis Program.[19]
- Continued to grow TSA's social media presence in 2017. TSA's Instagram account has more than 840,000 followers and was one of five nominees for two prestigious Webby Awards next to the likes of Conan O'Brien and The Onion. The main Twitter account shared 1,100 tweets, resulting in more than 31 million impressions and over 206,000 followers. In November, TSA officially launched a Facebook page and broadcasted its first *Ask Me Anything* on Facebook Live with more than 5,000 views.

Table 6: Freight Rail Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attack and enhance system resilience
<u>Overall Assessment</u>: Federal security partners and industry stakeholders continue to sustain a risk-based security posture. Freight railroads continue to sustain the reductions in risk associated with the transportation of Rail Security-Sensitive Materials (RSSM) that have been achieved over the last decade. The application of risk-based priorities including planning, training, exercises, risk reducing practices, information sharing, community outreach, and critical infrastructure protection has enabled the freight railroads to reduce the risks to their operations and the national freight rail network.
Objective 1: Sustain effective security plans through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences
Activity: Develop, periodically review, and update security plans based on available information. **Key Accomplishment**: One hundred percent of railroads that transport RSSM through High Threat Urban Areas (HTUA) reported having security plans and contingency preparations to implement enhanced risk mitigating measures at elevated terrorism alert levels.
Objective 2: Provide effective training for railroad frontline employees
Activity: Conduct training of frontline employees to identify, prevent, deter, and respond to

[19] Privacy documents for TSA listed at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

threats.

Key Accomplishments:

- Approximately 80,000 frontline employees of Class I railroads received or participated in security awareness training, which is approximately 49 percent of the total Class I Railroad workforce.[20]
- Distributed 17,590 freight railroad-specific and cyber counterterrorism guides to industry stakeholders in continued effort to enhance the recognition of indicators of possible terrorist activity.
- Adjudicated comments for the Security Training Surface Transportation Employees NPRM. The Final Rule is on the DHS Unified Agenda to be published in 2018, subject to regulatory reform requirements under Executive Order 13771, Reducing Regulation and Controlling Regulatory Costs.
- Adjudicated comments on the Surface Transportation VASP ANPRM.

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Railroads either conduct or participate in exercises designed to evaluate the preparedness for, and response to, security events.

Key Accomplishments:

- The Class I railroads conducted and participated in over 200 exercises focused on preparedness to address general or specific threats and security-related incidents or contingencies.
- Facilitated the use of the Simulation Deck platform during the Association of American Railroads' annual security exercise, which added real-world feel by injecting simulated media (video, radio, blogs, and social media) into the exercise environment.

Objective 4: Maintain and enhance programs to appropriately secure critical railroad physical and cyber infrastructure

Activity: Establish or update criteria to identify which infrastructure is most critical, and enhance programs to appropriately secure railroad critical infrastructure.

Key Accomplishments:

- Completed data collection and review of bridge and tunnel assessments since 2009 and initiated a process to update key information about bridges.
- Continued to improve three test beds, including freight rail bridges and the infrastructure protection projects in northern New Jersey. Continued outreach to the

[20] The Class I Railroads workforce is approximately 163,494 people; however, the entire workforce is not considered "front-line" employees that require training.

surface transportation industry to provide data and information gleaned from those initiatives.

- Mitigated current threats and vulnerabilities using RMAST activities, which typically include TSA Surface Transportation Security Inspectors (TSIs) discussing security awareness issues with stakeholder security and operational personnel.

Objective 5: Maintain operational procedures for reducing the risk associated with the transportation of passengers and materials of concern

Activity: Railroad carriers and shippers and receivers of RSSM continue to apply measures that mitigate security risks of the HTUA transportation of these materials.

Key Accomplishments:

- Conducted 2,672 inspections for compliance with the RSSM chain of custody regulations, indicating an industry compliance rate of 99.52 percent. The railroads, as required by 49 C.F.R. 1580.107, continued to apply operational measures that reduce the vulnerability of RSSM transiting one or more HTUAs. These measures include inspecting RSSM cars and securing exchange of custody at points of origin, interchange with other railroads, and points of delivery.
- Monitored the attendance of rail tank cars containing toxic inhalation hazard (TIH) materials being temporarily held or stopped in HTUAs. Conducted 9,338 observations of TIH tank car attendance, indicating an industry attendance rate of 99.02 percent.

Goal 2: Enhance effective domain awareness of transportation systems and threats

<u>**Overall Assessment**</u>: TSA and its Federal partners worked with industry organizations, such as the Railway Alert Network, to ensure rail security coordinators were provided with a variety of informational products to provide continuous awareness and assist in strategic and tactical planning for existing and emerging threats. Many of these products serve as the basis for educational and training materials for frontline employees. TSA routinely provides information on both kinetic and cyber threats to the railroad operators. TSA also regularly participates in the Association of American Railroads Rail Security Working Committee meetings.

Objective 1: Maintain and enhance mechanisms for information and intelligence sharing between the railroad industry and government

Activity: Ensure delivery of timely, meaningful, and actionable intelligence and security information products to rail security coordinators.

Key Accomplishments:

- Distributed more than 60 separate security information and intelligence products to designated rail security coordinators and security partners, including those produced by TSA, other DHS components, and Federal agencies. Examples of information and intelligence products include TSA Modal Threat Assessments, SAMs, Transportation

Intelligence Notes, and DHS Joint Intelligence Bulletins.

- Provided monthly reports analyzing "significant security concerns"[21] made by railroads and summarized them to provide quarterly reports with trend analysis.
- Maintained and managed a database of Rail Security Coordinators for freight railroads, hazardous materials shippers, and hazardous materials receivers.

Objective 2: Engage with first responders and the public to provide awareness of security concerns associated with railroad operations to promote situational security awareness and preparedness

Activity: Conduct activities and information sharing with law enforcement, public safety, and the general public that improve security awareness and understanding of the railroad's operations.

Key Accomplishment: Reported over 5,000 security awareness engagements that include interactions with law enforcement, emergency responders, and the public in their operating areas.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce

Overall Assessment: The FR mode continued to focus on safeguarding privacy and developing policy consistent with applicable privacy, civil liberties, and civil rights laws by conducting privacy impact assessments and addressing privacy complaints. TSA's social media customer service program provided timely information, improved customer service, and useful interactions with the American people. This award-winning outreach program is designed to better inform travelers of security initiatives, thereby reducing their stress and improving the security process.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishments:

- Evaluated all field activities to ascertain compliance with established laws, regulations, and policy.
- Performed significant outreach and training to educate field operations on transgender issues.

[21] Pursuant to 49 C.F.R. part 1580

- Published a Privacy Impact Assessment (PIA) for the TSA Contact Center, as a standalone from the DHS General Contact Lists PIA, and updated the PIA for the Encounters Analysis Program.[22]
- Continued to grow TSA's social media presence in 2017. TSA's Instagram account has more than 840,000 followers and was one of five nominees for two prestigious Webby Awards next to the likes of Conan O'Brien and The Onion. The main Twitter account shared 1,100 tweets, resulting in more than 31 million impressions and over 206,000 followers. In November, TSA officially launched a Facebook page and broadcasted its first *Ask Me Anything* on Facebook Live with more than 5,000 views.
-

Table 7: Highway and Motor Carrier Progress Assessment

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience

Overall Assessment: TSA collaborates with Highway and Motor Carrier (HMC) owners and operators to identify risks to critical systems and services, and aid in implementing risk-mitigating policies and programs to address gaps that may exist. BASE reviews of the largest trucking carriers, motorcoach operators, and pupil transportation operations further help stakeholders to understand and close security gaps in their systems. Exercise programs are essential to assist operators in directing their resources and efforts toward effective risk reduction. TSA facilitates I-STEP exercises to help HMC entities test and evaluate their security plans. In addition, EXIS, a TSA-sponsored online exercise tool, guides government and industry users through the exercise planning process and provides resources to design, document, and evaluate exercises for all transportation modes. Training resources, including the First Observer Plus™ security training program and Counterterrorism Guides, aid in informing a large percentage of the HMC employee population of security responsibilities and actions to identify and report security concerns.

Objective 1: Sustain effective security plans through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences

Activity: Develop vulnerability assessments and security planning guidance and tools for use by operators.

Key Accomplishment: Completed 126 (25 trucking; 12 school bus; 54 school district; 24 over-the-road bus (OTRB); and 11 OTRB terminal) BASE assessments that provide a random sample of operators' voluntary implementation of recommended security measures. Due to the HMC mode's large number of operators, TSA conducted random assessments to

[22] Privacy documents for TSA listed at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

identify progress and need-to-improve areas in security plans.

Objective 2: Provide effective training for highway frontline employees

Activity: Develop training resources and tools for use by operators based on identified needs (i.e., vulnerabilities, threat indicators, threat incident response protocols).

Key Accomplishments:

- Assisted with the development and publication of the mode-specific *First Observer Plus* ™ modules for highway sub-modes. Delivered *First Observer Plus* ™ training to the following industry stakeholders:
  - TCW, Inc. trucking company, January 2017
  - United Motorcoach Association (UMA), February 2017
  - Glendale, AZ School District, February 2017
  - National Center for Spectator Sports Safety and Security, February 2017
  - American Society of Safety Engineers (ASSE), March 2017
  - Detroit Area Parking Operators and Arena/Stadium Security Representatives, March 2017 (included train-the-trainer sessions)
  - International Parking Institute (IPI), May 2017 (included train-the-trainer sessions)
  - California Bus Association, August 2017
  - Orlando OTRB Operators and TSA Inspectors, September 2017 (included train-the-trainer sessions)
  - International Pipeline Forum, October 2017
  - Julliard School, Long Island Transportation, November 2017
- Published *Vehicle Ramming Attacks* guidance in May 2017, which is the first comprehensive analysis of this rapidly-spreading threat.
- Adjudicated comments for the Security Training Surface Transportation Employees NPRM. The Final Rule is in departmental review and is on the DHS Unified Agenda, subject to regulatory reform requirements under Executive Order 13771, Reducing Regulation and Controlling Regulatory Costs.
- Adjudicated comments on the Surface Transportation VASP ANPRM.
- Provided HMC Toolkit, HMC Counterterrorism Guides (19,352 school bus; 4,721 OTRB; 13,594 trucking; and 9,980 highway infrastructure), active shooter response cards, and terrorism indicator cards to industry stakeholders as part of a cooperative effort to improve HMC security.

Objective 3: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

Activity: Use exercise program to evaluate the resilience of OTRB operations to terrorist attacks.

Key Accomplishment: Completed six I-STEP exercises in Kansas City, KS; New Orleans, LA; Northern Virginia; Schaumburg, IL; Peoria, IL; and Houston, TX. In addition, TSA conducted on-site industry partner EXIS enrollments at each location and identified best practices from each exercise.

Objective 4: Maintain and enhance programs to appropriately secure critical physical and cyber infrastructure

Activity: Coordination and collaboration with industry to identify both physical and cyber vulnerabilities.

Key Accomplishments:

- Provided cybersecurity toolkit and other cyber security information throughout the HMC stakeholder community.
- Conducted 345 RMASTs, which is designed to mitigate threats and vulnerabilities, and typically include TSA Surface TSIs providing and discussing DHS/TSA-developed security-related materials with stakeholder personnel.
- Completed distribution of all TSA and Army Corps bridge and tunnel assessments and final reports, including classified appendices where appropriate, to state homeland security directors and DOTs.

Objective 5: Maintain operational procedures for reducing the risk associated with the transportation of passengers and materials of concern

Activity: Continuous development of options to mitigate potential threats to HMC operations.

Key Accomplishment: Provided relevant counterterrorism information to stakeholders along with security tools and resources to mitigate potential threats, including six I-STEP exercises and the distribution of HMC security resources, such as the HMC Toolkit, HMC Counterterrorism Guides (19,352 school bus; 4,721 OTRB; 13,594 trucking; and 9,980 highway infrastructure), active shooter response cards, and terrorism indicator cards.

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: TSA continued to develop highly cooperative stakeholder relationships by expanding domain awareness training and information sharing activities. It routinely provides information on both kinetic and cyber threats to the HMC industries. TSA also routinely participates in industry events and on security committees to raise the level of awareness and provide security tools and resources to private entities for implementation.

Objective 1: Maintain and enhance the mechanisms for information and intelligence sharing between the highway and motor carrier industry and government

Activity: Evaluate and improve the quality of intelligence and information products and the unclassified information delivery system provided to the HMC operators and infrastructure owners.

Key Accomplishments:

- Conducted quarterly conference calls providing stakeholders with current intelligence and threat briefs, updates on programs and policies, and an opportunity for stakeholder questions and comments.
- Issued 14 SAMs to industry during times of heightened alert or in response to real world terrorism events, providing security information and awareness information that emphasize threat-specific existing security measures and/or recommend voluntary protective measures.
- Conducted stakeholder follow-up calls with all modal stakeholders in the wake of significant terrorist attacks overseas. Each call included current threat and technique analysis and opportunity for stakeholder questions and input.
- Sponsored the delivery of daily reports to stakeholders through the Public Transit-Surface Transportation-OTRB Information Sharing and Analysis Center.

Objective 2: Engage with first responders and the public to provide awareness of security concerns associated with highway operations, and to promote situational and security awareness, and preparedness. Use the TSA Intermodal Security Training and Exercise Program and Exercise Information System programs to identify lessons learned and promote risk reduction activities throughout the highway and motor carrier landscape.

Activity: Conduct effective exercises with both private and public partners in high-risk areas by employing realistic threat scenarios that evaluate and identify opportunities to improve security resilience.

Key Accomplishments:

- Planned, budgeted, and executed six I-STEP exercises with local, state, and Federal law enforcement and first responder entities. Locations included:
  - Kansas City, KS (school bus)
  - New Orleans, LA (all modes)
  - Northern Virginia (trucking)
  - Schaumburg, IL (Chicago metro area) (trucking)
  - Peoria, IL (school bus)
  - Houston, TX (highway infrastructure)
- Provided security awareness and TSA security initiative updates at more than 21 public/private stakeholder events/calls.
- Coordinated with the DHS Office for State and Local Law Enforcement to develop the SETA pilot program, which simulates coordinated terrorist attacks by covertly placing unattended bags/suspicious bags on multiple transit vehicles simultaneously. In 2017, two SETA activities were conducted on school districts.
- Distributed bridge and tunnel vulnerability reports generated by the U.S. Army Corps of Engineers project to state homeland security directors, state departments of transportation homeland security officers, and to the Transportation Research Board within the National Academy of Sciences, for use as guidance in construction of new

bridges and tunnels.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: The HMC mode continued to consider the privacy, civil liberties, and civil rights of individuals and corporations in developing and implementing policies and processes ensuring the freedom of movement of people and commerce. All related HMC risk-based security initiatives and activities were evaluated to ensure compliance with established standards and policy. Additionally, HMC stakeholders responded well to voluntary participation in BASE assessments with the assurance that findings and recommendations are closely held under Sensitive Security Information standards or, where appropriate, classified information policies. BASE assessments and U.S. Army Corp of Engineers structural visits are scheduled to ensure the flow of commerce is not interrupted.

Objective 1: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishments:

- Evaluated all field activities to ascertain compliance with established laws, regulations, and policy.
- Performed significant outreach and training to educate field operations on transgender issues.
- Published a Privacy Impact Assessment (PIA) for the TSA Contact Center, as a standalone from the DHS General Contact Lists PIA, and updated the PIA for the Encounters Analysis Program.[23]
- Continued to grow TSA's social media presence in 2017. TSA's Instagram account has more than 840,000 followers and was one of five nominees for two prestigious Webby Awards next to the likes of Conan O'Brien and The Onion. The main Twitter account shared 1,100 tweets, resulting in more than 31 million impressions and over 206,000 followers. In November, TSA officially launched a Facebook page and broadcasted its first *Ask Me Anything* on Facebook Live with more than 5,000 views.
-

Table 8: Pipeline Progress Assessment

Goal 1: Manage risks of terrorist attacks and enhance systems resilience

[23] Privacy documents for TSA listed at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

Overall Assessment: TSA worked with government and industry stakeholders to secure the Nation's pipeline systems from terrorist attacks through voluntary security program implementation, robust industry engagement, and collaborative technology test beds. TSA industry security partners continued to use the Critical Facility Security Review (CFSR) and Corporate Security Review (CSR) programs to assess risk throughout the operating environment of the top 100 critical pipeline systems. Both programs highlight stakeholder opportunities to implement the 2011 TSA Pipeline Security Guidelines and share industry smart/best practices. Additionally, plans designed to enhance CSR delivery reached fruition as TSA secured a new contract to support CSR execution and analysis. TSA worked with stakeholders to implement the NIST Cybersecurity Framework through industry engagement in drafting an update to the TSA Pipeline Security Guidelines.

Objective 1: Maintain operational protocols for reducing the risk associated with the transmission through pipelines of natural gas, hazardous liquids, and materials categorized as toxic inhalation hazards

Activity: Strategically integrate TSA Pipeline Security Guidelines throughout the security operations environment of industry partners owning and operating our Nation's most critical natural gas and hazardous liquid pipeline systems by continued engagement of the CSR and CFSR programs and related processes.

Key Accomplishments:

- Engaged with stakeholders through the CSR and CFSR programs and process to collaboratively integrate TSA Pipeline Security Guidelines throughout the industry's security operations environment at the top 100 critical pipeline systems.
- Continued two pipeline site security technology test beds, including advanced infrastructure protection technologies.

Objective 2: Enhance cybersecurity of the pipeline critical infrastructure

Activity: Conduct outreach with pipeline industry stakeholders on the voluntary implementation of the principles and best practices of risk management through the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Key Accomplishments:

- Conducted significant outreach to industry stakeholders in drafting an update to the TSA Pipeline Security Guidelines, including integration of the NIST Cybersecurity Framework.
- Continuing a pilot program initiated in 2016, conducted cyber assessment reviews at one pipeline company, in collaboration with the Federal Energy Regulatory Commission.

Goal 2: Enhance effective domain awareness of transportation systems and threats

Overall Assessment: TSA's strong stakeholder engagement program remained focused on delivering value-added situational awareness messages, intelligence briefings, and other information sharing products through a trusted, effective network consisting of pipeline industry and government partners. In addition, TSA uses these same information sharing networks to:

- Coordinate and deliver training;
- Coordinate security exercises, assessments, and reviews;
- Deliver industry-specific training materials such as Pipeline Counterterrorism Guides,and online resources;
- Share smart/best practices; and
- Share security guidelines.

As prescribed in the DHS National Infrastructure Protection Plan, TSA relies on the Critical Infrastructure Partnership Advisory Council (CIPAC) process to facilitate government and industry information and intelligence sharing and security planning, coordination, and execution. Under the CIPAC, TSA actively participates with the Oil and Natural Gas Sector Coordinating Council and Energy Government Coordinating Council regarding intelligence and information sharing, pipeline security strategies, policies, activities, capability gaps, technology initiatives, and related issues. In addition, TSA continued to work collaboratively with the Canadian Government (Natural Resources Canada) on matters of mutual interest including information sharing and industry outreach.

Objective 1: Enhance the means to share information and intelligence between the pipeline industry and government

Activity 1: Assess opportunities for enhanced information sharing processes with the natural gas and hazardous liquid pipeline community through industry-developed activities such as Information Sharing and Analysis Centers.

Key Accomplishment: Continued outreach to the pipeline industry, including distribution of information regarding surface transportation security and cyber incidents.

Activity 2: Deliver timely, meaningful, and actionable security information products to pipeline industry security coordinators.

Key Accomplishments*:*

- Provided seven unclassified threat briefings to industry representatives during monthly pipeline security conference calls.
- Continued distribution of a Pipeline Counterterrorism Guide as requested by industry stakeholders.

Objective 2: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience

~~WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

Activity: Test and improve resilience to terrorist attacks by collaborating with stakeholders to develop Pipeline Industry-specific I-STEP exercises featuring key DHS/TSA risk reduction areas of consideration such as supply chain disruption.

Key Accomplishments:

- Collaborated with industry to plan, develop, and deliver one I-STEP exercise based on overarching TSA risk mitigation and resilience strategies and plans.
- Conducted 29 RMASTs to mitigate current threats and vulnerabilities for the pipeline industry. The RMAST activities typically include TSA Surface TSIs providing and discussing the following DHS/TSA-developed security-related materials with stakeholder personnel:
  - Pipeline Counterterrorism Guide;
  - Surface Transportation Cybersecurity Awareness Guide;
  - Pipelines: Countering Improvised Explosive Devices DVDs;
  - Protecting Pipeline Infrastructure: The Law Enforcement Role DVD;
  - Good Neighbors: A Pipeline Security Neighborhood Watch brochure;
  - Pipeline Security Awareness for Employees brochure; and
  - *First Observer Plus* ™ Security Awareness Training Program.

Objective 3: Work with industry stakeholders and encourage them to engage with first responders and the public to understand community concerns and resilience needs, to provide awareness of pipeline security issues, and to promote system preparedness and resilience

Activity: Maintain and enhance commitment to sustained engagement with first responders, customers and the public to provide awareness of security concerns and preparedness measures.

Key Accomplishment: Collaborated with industry to plan, develop, and deliver one I-STEP exercise based on overarching TSA risk mitigation and resilience strategies and plans.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

<u>Overall Assessment</u>: TSA continued to consider the privacy, civil liberties, and civil rights of individuals and corporations in developing and implementing policies and processes ensuring the freedom of movement of people and commerce. All related pipeline risk-based security initiatives and activities were evaluated to ensure compliance with established standards and policy.

Objective: Protection of civil liberties and freedom of movement of people and commerce

Activity: Develop policy consistent with applicable privacy, civil liberties, and civil rights laws, regulations, and policies.

Key Accomplishment: Considered applicable privacy, civil liberties, and civil rights laws, regulations, and policies in drafting an update to the TSA Pipeline Security Guidelines, which were developed collaboratively with industry.

D. Intermodal

The Intermodal Security Subsector covers the transportation elements of the global supply chain and the delivery of goods from origin to destination by multi-modal postal and parcel shipping services. The global supply chain consists of a dense network of routes and carriers operating efficiently to provide time-sensitive deliveries. Threats to intermodal transportation links of the supply chain are the same as those for the individual modes serving the supply chain. The threats also include the potential delivery of explosives, dangerous chemicals, or biological agents to specific targets. While the direct consequences of attacks on intermodal transportation systems may be limited, the indirect costs of attack-related disruptions could have significant and lasting effects, particularly where shipping options are limited.

Table 9: Intermodal Progress Assessment

Goal 1: Enhance resilience of the global transportation supply chain system
<u>**Overall Assessment:**</u> The sector continues to collaborate with industry stakeholders and security partners on supply chain issues and innovative approaches to security. TSA participated in a policy development process with industry engagement and the Compliance Security Enhancement Through Testing Program to enhance industry compliance through measures other than penalties. In addition, the subsector coordinated U.S. and international positions on cargo technological standards, supply chain security, and advance cargo information with international cargo security working groups, such as the ICAO's Aviation Security Panel.
Objective 1: Reduce systemic risk of a supply chain disruption prior to a potential nationally significant event by using layered risk management principles **Objective 2: Improve capacities to effectively collect, protect, analyze, and share supply chain information among stakeholders, and strengthen and grow stakeholder partnerships and collaboration** **Objective 3: Ensure orderly resumption of commerce following a large-scale disruption**
Activities: • Assure compliance with international security protocols such as the International Ship and Port Facility Security Code.

- Implement the International Port Security Program to assess the effectiveness of anti-terrorism measures in foreign ports, build security capacity where gaps exist, and impose conditions of entry on vessels arriving in the United States from ports with substandard security.
- Conduct exercises of the National Response Framework, the Response Federal Interagency Operational Plan, and other related all hazards and security incident response plans to enhance resumption of trade following a large-scale disruption.

Key Accomplishments:

- Conducted DHS-led regional assessments using the Regional Resilience Assessment Program to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen infrastructure resilience. Key findings concentrate on regionally significant issues and present options to enhance resilience.
- The USCG conducted over 5,900 MTSA facility inspections, which aim to prevent maritime transportation security incidents and marine casualties resulting from malicious acts, accidents, or acts of nature against waterfront facilities.
- I-STEP engaged with over 33 stakeholder groups to conduct seven multiple intermodal security exercises, resulting in after-action reports and development of industry practices.

Goal 2: Enhance the efficient and secure movement of goods

Overall Assessment: The Air Cargo Advance Screening (ACAS) Pilot Program, initiated in 2010, allows TSA inspectors to work with CBP officers to identify high-risk air cargo shipments, facilitating targeted, enhanced screening prior to loading on board U.S.-bound aircraft. TSA and CBP held multiple meetings with industry stakeholders to discuss requirements, regulations, lessons-learned, and progress toward implementation. TSA and CBP continued to jointly develop a rulemaking to replace the ACAS Pilot Program with a permanent ACAS requirement, which was issued in 2018.

Objective 1: Mitigate and manage risks as early as possible in the global supply chain networks to promote the efficient flow of commerce

Activities:

- Apply risk based methods to focus security resources on higher risk cargos (Automated Targeting System, Automated Manifest System, Air Cargo Advance Screening, and Customs-Trade Partnership Against Terrorism[24]).
- Implement advance notice of arrival protocols including CBP's 24-Hour Advanced Manifest Rule and the USCG's 96-Hour Advance Notice of Arrival to identify higher risk cargo movements for enhanced security review.

[24] Additional information on these program is available on https://www.dhs.gov.

- Enhance Air Cargo Security Programs: require shippers, air forwarders, independent facilities, and airlines to screen cargo before it is loaded aboard aircraft.

Key Accomplishments:

- The ACAS pilot was extended through 2017 to allow additional time for the two lead agencies, CBP and TSA, to develop a final rule.
- TSA enrolled approximately 505,000 workers in the *TWIC*® program,[25] for a program total of 3.6 million. The *TWIC*® program provides a security threat assessment and tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, vessels regulated under the MTSA, and all USCG-credentialed merchant mariners.
- CBP prescreened over 80 percent of all maritime containerized cargo imported into the United States at 58 operational Container Security Initiative ports.
- Conducted security threat assessments on more than 250,000 truck drivers, vetting applicants against criminal, immigration, and intelligence databases for Hazardous Materials Endorsements issued by State motor vehicle agencies, for a total enrollment of 3 million.
- Enrolled approximately 273,000 people in the Hazardous Materials Endorsement Threat Assessment Program for a total enrollment of 3 million.
- The USCG conducted over 5,900 MTSA facility inspections, which aim to prevent maritime transportation security incidents and marine casualties resulting from malicious acts, accidents, or acts of nature against waterfront facilities.

Objective 2: Enhance implementation of global supply chain-related standards, best practices, and guidelines and regulations allowing stakeholders to realize efficiencies while maintaining acceptable levels of security

Activity: Implement Customs-Trade Partnership Against Terrorism to improve the security of private companies' supply chains with respect to terrorism.

Key Accomplishments:

- Used Pre-Loading Advance Cargo Information to examine the application of advanced cargo information and as a platform for dialogue among pilot program participants and between regulators and industry.
- Collaborated with the ICAO Aviation Security Panel Working Group on Air Cargo on the concept of best practices or similar material that may be appropriate for the ICAO to develop. This material would include the use of Pre-Loading Advance Cargo Information for aviation security purposes for those states considering using air cargo information for targeting.

[25] Required by the Maritime Transportation Security Act (Pub.L. 107–295) for workers who need unescorted access to secure areas of the nation's maritime facilities and vessels.

Objective 3: Improve situational awareness of terrorist threats to the global supply chain

Activity: Work with other DHS Components, DOT, the Department of Energy, the Department of Justice, the Office of the Director of National Intelligence, the Department of Defense, and industry to develop cyber risk assessment capabilities.

Key Accomplishments:

- Continued to work closely with industry to encourage adoption of the NIST Cybersecurity Framework and issued the Transportation Systems Sector Cybersecurity Framework Implementation Guidance document.
- Strengthened cybersecurity information sharing via the Government and Sector Coordinating Councils, including associated sector cyber working groups
- Participated in the Aviation Cybersecurity Initiative, a Tri-Chair interagency working group, led by FAA, DHS, and DOD, that is identifying potential cybersecurity vulnerabilities in aviation, developing cyber risk assessment programs, and researching technical solutions to mitigate any identified vulnerabilities.
- Conducted surface transportation assessment programs that include both physical cyber risk management concepts.
- Participated in a DHS Cybersecurity Integrated Project Team process researching high-priority technology solutions.

Objective 4: Improve industry involvement in the global supply chain Research and Development process to improve security of goods in transit and minimize delays

Activity: Improve industry participation in development of the Cargo and Supply Chain R&D Plan.

Key Accomplishments:

- The joint Transportation Sector R&D Working Group and DHS Integrated Project Team on Aviation Security identified capability gaps and recommended priority R&D projects for consideration by DOT and by DHS Science and Technology Directorate.
- The joint Surface Transportation Systems R&D Working Group, including DHS, DOT, and public and private partners, identified security capability gaps in the surface modes of transportation, which serve as a basis for developing R&D project requirements for consideration by the funding organization.
- Continued to enhance industry participation in the development of the National Strategy For Transportation Security, and in support of the DHS Directorates for Science and Technology, and National Protection and Programs, the National R&D Plan, and the National Infrastructure Protection Plan.

Objective 5: Enhance the security of critical infrastructure and conveyances in order to protect the supply chain and nodes against terrorist attacks

Activity: See activities in the 2016 NSTS Modal Security Plans.

Key Accomplishment: Maintained robust formally established marketplace-based technology assessments and formally established test beds in collaboration with transportation operators.

Table 10: Postal and Shipping Progress Assessment

Goal 1: Manage risks to the P&S Subsector and enhance system resilience

Overall Assessment: The Postal and Shipping (P&S) Subsector continues to remain vigilant to ensure the continuity of operations, ease of use, and public confidence by creating a multi-layered security posture that integrates public and private partners and protective measures to deny adversaries the ability to exploit the subsector and its customers.

Objective 1: Improve deterrence and response to a national or regional terrorist emergency affecting the P&S Subsector

Activity: Improve risk assessment processes.

Key Accomplishments:

- U.S. Postal Inspection Service (USPIS) employees conducted 735 postal facility reviews using the Vulnerability Risk Assessment Tool, a comprehensive, risk-based model that identifies security deficiencies.
- In 2017, USPIS worked with state, federal, and local law enforcement partners to provide mail screening at eight national mail screening events to include Super Bowl LI. More than 17,000 mail pieces and private courier deliveries were screened at the events, heightening safety and security for all.

Objective 2: Minimize the risk of unauthorized individuals gaining access into secured areas

Activity: Expand voluntary use of best practice security protocols.

Key Accomplishment: Conducted 735 postal facility reviews using the Vulnerability Risk Assessment Tool, a comprehensive, risk-based model that identifies security deficiencies.

Goal 2: Enhance effective domain awareness of P&S systems and threats

Overall Assessment: The P&S Subsector ensures continuity of operations by providing incident reporting mechanisms and awareness/outreach programs with law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the subsector. These activities ensure timely, relevant, and accurate threat reporting from law enforcement and intelligence communities to key decision makers in the sector in order to implement appropriate threat-based security measures and risk management programs. The community is linked through the Homeland Security Information Network (HSIN).

Objective 1: Improve awareness of cross sector interdependencies

Activity: Partner with industry and the Intelligence Community to facilitate threat awareness. Use the HSIN to communicate with the P&S community to retrieve updated information and intelligence. Work to develop a communications procedure for routine and incident-specific information sharing.

Key Accomplishment: TSA worked with industry partners to understand the threat, maintain awareness of vulnerabilities, and encouraged the industry to implement industry leading practice mitigation strategies. TSA continued to enhance domain awareness with security partners and stakeholders at open-forum meetings of P&S community.

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce

Overall Assessment: The P&S subsector processed 154.3 billion letters and parcels, and delivered them to more than 156 million addresses in every state, city, and town in the country. USPIS provided security for these mail pieces from their entry into the postal network to their destinations. Federal law forbids tampering with the mail; only the person to whom a mail piece is addressed may open it. Postal Inspectors have the investigative jurisdiction in cases where mail delivery is interrupted by theft, riffling, obstruction, or destruction. Through enforcement measures and educational programs, USPIS is thwarting crime and keeping the mail safe and secure.

Objective 1: Minimize the security risks and delays in freight movement, and reduce potential for adverse privacy, civil rights, and civil liberty impacts of security policies

Activity: Enhance continuity of operations plans to ensure the sector identifies and protects privacy, civil rights, and civil liberties in the free movement of parcels to intended recipients.

Key Accomplishments:

- USPIS completed a five-year initiative for the Consumer Alert News Network, educating the public with fraud awareness messages.Teamed with the American Association of Retired Persons, USPIS launched *Operation Protect Veterans*, a campaign focused on making veterans aware of frauds and crimes against them.

~~**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.~~

Appendix A: Acronym List

Acronym	Definition
ACAS	Air Cargo Advance Screening
ADIAC	Aviation Domain Intelligence Integration and Analysis Cell
AMSTEP	Area Maritime Security Training and Exercise Program
ANPRM	Advance Notice of Proposed Rule Making
APTA	American Public Transportation Association
BASE	Baseline Assessment for Security Enhancements
CATA	Cities and Airports Threat Assessment
CBP	U.S. Customs and Border Protection
CFSR	Critical Facility Security Review
CIPAC	Critical Infrastructure Partnership Advisory Council
CSR	Corporate Security Review
CT	Counter Terrorism
CTC	Canine Training Center
DHS	Department of Homeland Security
DOT	Department of Transportation
DVD	Digital Video Disc
ETD	Explosive Trace Detection
EXIS	Exercise Information System
FAA	Federal Aviation Administration
FATA	Foreign Airport Threat Assessment
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FR	Freight Rail
FY	Fiscal Year
GCC	Government Coordinating Council
HIP	USCG Homeport Internet Portal
HMC	Highway and Motor Carrier
HSIN	Homeland Security Information Network
HTUA	High Threat Urban Area
ICAO	International Civil Aviation Organization
IPS	International Port Security
I-STEP	Intermodal Security Training and Exercise Program
ITF	Innovation Task Force
MAP	Management, Administration, and Professional
MTPR	Mass Transit and Passenger Rail
MTS	Maritime Transportation Security
MTSA	Maritime Transportation Security Act

NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
NPRM	Notice of Proposed Rule Making
NSTS	National Strategy for Transportation Security
NVIC	Navigation and Vessel Inspection Circular
ODNI	Office of the Director of National Intelligence
OTRB	Over the road bus
P&S	Postal and Shipping
PT-ISAC	Transit and Rail Intelligence Awareness Daily Report and Analysis Center
R&D	Research and Development
RAILSAFE	Regional Alliance Including Local, State, and Federal Efforts
RCTIC	Radiological Nuclear Detection Concepts, Tactics and Integration Course
RMAST	Risk Mitigation Activities for Surface Transportation
RSSM	Rail Security-Sensitive Materials
SAM	Security Awareness Message
SCC	Sector Coordinating Council
SETA	Security Enhancement Through Assessments
TIH	Toxic Inhalation Hazard
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSGP	Transportation Security Grant Program
TSI	Transportation Security Inspectors
TSO	Transportation Security Officer
TSSRA	Transportation Sector Security Risk Assessment Cities and Airports Threat Assessment
TTAL	Top Transit Asset List
TWIC®	Transportation Worker Identification Credential
USCG	United States Coast Guard
USPIS	U.S. Postal Inspection Service
VASP	Vulnerability Assessments and Security Plans
VIPR	Visible Intermodal Prevention and Response

Appendix B: Legislative Language: Annual Reporting Requirements

The Annual Report on Transportation Security covers four annual reporting requirements, including implementation of the National Strategy for Transportation Security, the Transportation Systems Sector-Specific Plan, and other statutory requirements, as detailed below, to achieve efficiency and deliver a coordinated message to the White House and Congress. This report satisfies the following reporting requirements:

1. **Annual Periodic Progress Report on the National Strategy for Transportation Security: 49 U.S.C. § 114(s)(4)(C):**
   Periodic progress report –

   (i) Requirement for report. - Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, United States Code, the Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

   (ii) Content. - Each progress report submitted under this subparagraph shall include, at a minimum, the following:

   (I) Recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

   (II) An accounting of all grants for transportation security, including grants and contracts for research and development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the goals of the National Strategy for Transportation Security.

   (III) An accounting of all –

   (aa) funds requested in the President's budget submitted pursuant to section 1105 of title 31 for the most recent fiscal year for transportation security, by mode;

   (bb) personnel working on transportation security by mode, including the number of contractors; and,

   (cc) information on the turnover in the previous year of senior staff of the Department of Homeland Security, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department.

2. **Annual Report on Transportation Security: 49 U.S.C. § 44938(a):**
(a) Submit to Congress a report on transportation security with recommendations the Secretary considers appropriate. The report shall include—
(1) an assessment of trends and developments in terrorist activities, methods and other threats to transportation;
(2) an evaluation of deployment of explosive detection devices;
(3) recommendations for research, engineering and development activities related to transportation security, with exceptions as noted in statute;
(4) identification and evaluation of cooperative efforts with other Federal entities;
(5) an evaluation of cooperation with foreign authorities;
(6) the status of the extent to which the recommendations of the President's Commission on Aviation Security and Terrorism have been carried out and the reasons for any delay in carrying out those recommendations;
(7) a summary of the activities of the Assistant Administrator for Intelligence & Analysis;
(8) financial and staffing requirements of the Assistant Administrator for Intelligence & Analysis;
(9) assessment of financial and staffing requirements, and attainment of existing staffing goals, for carrying out duties and powers of the TSA Administrator related to security; and
(10) appropriate legislative and regulatory recommendations.

3. **Annual Update on Enhanced Security Measures:** as required by Section 109(b) of the Aviation and Transportation Security Act (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296.

4. **Annual Report on the National Strategy for Public Transportation Security:** 6 U.S.C. § 1141:
(a) Annual report to Congress
(1) In general
Not later than March 31 of each year, the Secretary shall submit a report, containing the information described in paragraph (2), to the appropriate congressional committees.
(2) Contents
The report submitted under paragraph (1) shall include—
(A) a description of the implementation of the provisions of this subchapter;
(B) the amount of funds appropriated to carry out the provisions of this subchapter that have not been expended or obligated;
(C) the National Strategy for Public Transportation Security required under section 1133 of this title;
(D) an estimate of the cost to implement the National Strategy for Public Transportation Security which shall break out the aggregated total cost of needed capital and operational security improvements for fiscal years 2008–2018; and

(E) the state of public transportation security in the United States, which shall include detailing the status of security assessments, the progress being made around the country in developing prioritized lists of security improvements necessary to make public transportation facilities and passengers more secure, the progress being made by agencies in developing security plans and how those plans differ from the security assessments and a prioritized list of security improvements being compiled by other agencies, as well as a random sample of an equal number of large- and small-scale projects currently underway.

(3) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

5. **Annual Report on the National Strategy for Railroad Transportation Security:** 6 U.S.C. § 1161

(e) Report

(1) Contents

Not later than 1 year after August 3, 2007, the Secretary shall transmit to the appropriate congressional committees a report containing—

(A) the assessment and the National Strategy required by this section; and § 1162 TITLE 6—DOMESTIC SECURITY Page 2561 So in original. The word ''to'' probably should not appear.

(B) an estimate of the cost to implement the National Strategy.

(2) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate
or necessary.

(f) Annual updates

Consistent with the requirements of section 114(t) 1 of title 49, the Secretary shall update the assessment and National Strategy each year and transmit a report, which may be submitted in both classified and redacted formats, to the appropriate congressional committees containing the updated assessment and recommendations.

Appendix C: Public Transportation Security Annual Report 6 U.S.C. § 1141

This appendix addresses the annual reporting requirements of 6 U.S.C. § 1141, covering the implementation of the National Strategy for Public Transportation Security, as defined by Title 6-Domestic Security, Chapter 4-Transportation Security, Subchapter III-Public Transportation Security, Sections 1131 through 1139.

1) Description of the implementation of the provisions of Title XIV of the 9/11 Act (title)

§1131 Definitions

Status: No action required

§1132. Findings

Status: No action required

§1133. National Strategy for Public Transportation Security

Status: Implemented through the 2016 National Strategy for Transportation Security, Appendix D, Surface Security Strategies and Plan.

§1134. Security assessments and plans

Status: See 4) a) and 4) c) below. The comment period for the Advance Notice of Proposed Rulemaking on Surface Transportation Vulnerability Assessments and Security Plans closed May 15, 2017. TSA has reviewed the comments and is developing a notice of proposed rulemaking. See 81 FR 91401.

§1135. Public transportation security assistance

Status: See 2) below

§1136. Security exercises

Status: TSA's Intermodal Security Training and Exercise Program (I-STEP), a security exercise program designed to reduce risks to critical transportation infrastructure, collaborated with transportation operators and security partners to build and sustain security preparedness to protect the traveling public, enhance national resilience, and identify capability gaps and needed resources. In FY 2017, I-STEP collaborated with security partners to produce 33 transportation security exercises supporting all modes of transportation. Of these, 14 were in the public transportation sector. Over 815 external stakeholder organizations in total were engaged during exercises with surface transportation operators. Two key I-STEP exercises directly supported *TSA's Public Area Security National Framework* targeting development of strategies for incident management and identification of security areas requiring additional partnerships or resources to reduce security gaps. I-STEP followed up by helping Chicago Transit Authority develop a new Standard Operating Procedure (SOP) for Active Assailants and by helping Amtrak convene key stakeholders in NY and NJ to better understand security vulnerabilities between Penn Station and the Hudson Tunnel before major construction was undertaken in the summer of 2017.

§1137. Public transportation security training program

Status: The comment period for the Notice of Proposed Rulemaking on Security Training for Surface Transportation Employees closed March 16, 2017. The Final Rule is in departmental review and is on the DHS Unified Agenda, subject to regulatory reform requirements under Executive Order 13771, Reducing Regulation and Controlling Regulatory Costs. See 81 FR 91336.

§1138. Public transportation research and development

Status: To ensure market technology stimulation and maturation, TSA plans, develops, and executes assessment processes to determine innovative and emerging technology suitability, effectiveness, and feasibility in public areas and surface transportation venues. This includes laboratory-based evaluations and field assessments in areas such as anomaly explosive detection, intrusion detection, standoff detection, remote screening, and blast mitigation. TSA also coordinates Chemical-Biological and other Weapons of Mass Destruction technology-related activities with the DHS Science and Technology Directorate and other Federal departments and agencies. TSA coordinates and manages mass transit test beds with stakeholders and technology end-users to assess promising technology solutions and other tools to drive mission success, address current and emerging threats, close capability gaps, and reduce risk of serious disruptions to public area and transportation stakeholders. The data gathered from these test beds and the technologies used within them are a major factor in driving priorities in coordination with end-users. TSA collects and analyzes operational needs, technology requirements, and security concerns in collaboration with industry through the formally chartered R&D Working Group and in partnership with DHS Science and Technology. This group serves as the primary mechanism for gathering R&D input, which comes from transportation stakeholders such as DOT, DHS Science and Technology Directorate, the Department of Defense, and state and local representatives. TSA also establishes Integrated Project Teams, such as for Standoff Detection, to facilitate increased formal collaboration between key government organizations to enhance and mature standoff detection technologies.

Examples of large-scale projects include:

- Mass Transit Testbeds: Amtrak, Los Angeles Metro (CA), New Jersey Transit (NJ), Bay Area Rapid Transit (CA), and Washington Metropolitan Area Transit Authority (D.C.)
- Freight Rail Test Beds: Tennessee River Bridge (AL), Plattsmouth Bridge (NE), Hwy 1&9 (NJ), and Northern Branch Rail Corridor (NJ)
- Pipeline Test Beds: Yorktown Junction (VA), Linden (NJ), and a representative test fixture at the Johns Hopkins Applied Physics Laboratory (MD)

Examples of small-scale projects include:

- Special Studies: Blast Mitigation and Bus Studies

- o Representative National Special Security Events Support

§1139. Information sharing

Status: The PT-ISAC has provided the government and the commercial transportation industry with alerts, bulletins, information, and analysis concerning terrorist movements, operations, threats, and, on rare occasions, reports on suspicious sightings of possible terrorist activity. In turn, such information is jointly shared with TSA and an international association of over 1,500 public and private member organizations and stakeholders. The PT-ISAC functions as a sector-specific platform, providing critical information/intelligence requirements covering threats, incidents, and vulnerabilities facing the transportation sector.

2) Amount of funds appropriated to carry out the provisions of this title that have not been expended or obligated.

The TSGP is one of the Federal Emergency Management Agency's (FEMA) annual grant programs that directly support transportation infrastructure security activities. Section 1406 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53) (6 U.S.C. § 1135) authorized appropriations for TSGP through 2011. The *Department of Homeland Security Appropriations Act, 2017* (Pub. L. No. 115-31) provides the appropriation for it, though the program remains unauthorized for additional appropriations. The Table 1 below shows historic TSGP funding levels through FY 2017. As shown in Table 2, TSGP funding has been fully obligated to high-risk public transportation systems; but not all funds have been expended as the period of performance for the FY 2016, FY 2017, and FY 2018 grants is still open.[26]

Table 1

TSGP Totals		
2006-2017	$315M	TSGP funds awarded to Operational Activities
2006-2017	$487M	TSGP funds awarded to Operational Deterrence
2006-2017	$1.4B	TSGP funds awarded to Capital Projects

Table 2

Year of appropriation	**Funds appropriated & Awarded**	**Balance (funds remaining or open obligations)***
FY 2016	$87.0M	$53.0M
FY 2017	$88.0M	$73.9M
FY 2018	$88.0M	$88.0M

**Note: The balance amounts are current as of 10/31/18. The period of performance for these awards is thirty-six (36) months. In this context, it is important to note that transit systems often do not drawdown funds until a project is complete.*

[26] TSGP funding period of performance for expenditure is approximately 3 years from the fiscal year of obligation.

The 2017 Enacted Surface Appropriation funding appropriated to TSA for surface transportation-related security activities is reflected in Table 3 below:

Table 3

2017 Surface Appropriation:	
$32.2M	Surface Transportation Security Operations and Staffing
$91.5M	Surface Transportation Security Inspectors and Visible Intermodal Prevention Response (VIPR)
$15M	Surface Transportation Procurement Construction and Improvements
$138.7M	Total appropriation

3) Estimated cost to implement the National Strategy for Public Transportation Security that breaks out the aggregated cost of needed capital and operational security improvements for fiscal years 2008-2018.

The estimated aggregated cost of needed capital and operational security improvements was $6.4 billion for 2015, which is the last projected year in the American Public Transportation Association, Survey of United States Transit System Security Needs, Summary of Findings, dated April 2010.[27] According to the survey, the five-year security-related investment need estimate through 2015 included $4.4 billion for transit security-related capital investment, plus $2 billion for operational security improvements for 35 of its transit agency members, operating 43 percent of all transit vehicles that report in the Federal Transit Administration, National Transit Database and are TSGP eligible. The 2017 estimated adjusted cost to implement the NSTS for the entire high-risk public transportation agency population exceeds $4.7 billion.

4) State of public transportation security in the U.S., including:

a) The status of security assessments;

The voluntary BASE program was used to review security assessments conducted by public transportation agencies. Three-hundred and five BASE reviews were conducted between FY 2014 and FY 2017, including 61 on agencies that are in the high-risk category (defined by having an average weekday ridership of more than 60,000 passengers). All high-risk agencies (100 percent) had performed a security assessment of their systems.

b) Progress being made developing prioritized lists of security improvements to secure public transportation facilities and passengers;

TSA and FEMA developed funding priorities for the TSGP and have reviewed those priorities, adjusting as necessary. Agencies that submit applications that are not aligned

[27] APTA, Survey of United States Transit Systems Security Needs, Summary of Findings, April 2010. http://www.apta.com/gap/legissues/other/Documents/APTA%20Security%20Survey_April2010.pdf

with the funding priorities are not considered for funding. The prioritized funding has resulted in security improvements as projects are completed.

c) **Progress made by agencies developing security plans and how those plans differ from the security assessments;**

The BASE program assesses public transportation agencies against multiple security-related categories identified by the public transportation community as fundamental for a sound security program, including the presence and quality of a security plan and assessment. The results of the BASE assessments indicate gaps or shortfalls in existing plans and allow the agencies to adjust and strengthen their plans to close the gaps. There was a three percent increase over six years in high-risk agencies having security plans.

5) **A random sample of an equal number of large- and small-scale projects currently underway.**

Ongoing projects vary greatly both in type and size. Projects range from lower-dollar amount training, exercise, and public awareness projects, to operational deterrence projects to multi-million dollar infrastructure capital protection projects for stations, bridges, and tunnels.

Examples of large-scale projects currently underway include:

- Securing underground/underwater vulnerable points of entry at top transit asset list (TTAL) assets
- Perimeter Security at a large, multi-modal TTAL asset
- Physical barriers and electronic security measures at a bridge critical to mass transit operations
- Portable barrier systems at TTAL assets

Examples of small-scale projects currently underway include:

- Sustainment of K-9 teams, mobile screening teams, anti-terrorism teams, and directed/surge patrols on overtime
- *See Something, Say Something* ™ campaign, which was originally created with TSGP funds, and other public awareness campaign materials and resources
- Closed-circuit television and access control at transit stations and platforms

Message from the Administrator

December 19, 2017

I am pleased to present the following report, "Strategic Five-Year Technology Investment Plan Biennial Refresh," (Refresh) prepared by the Transportation Security Administration (TSA).

The Refresh was prepared pursuant to a requirement in Section 1611 of the *Homeland Security Act of 2002* (P.L. 107-296), as amended by Section 3 of the *Transportation Security Acquisition Reform Act* (P.L. 113-245). It presents an update to the original investment plan with particular emphasis on changes to the methodologies provided in the original Strategic Five-Year Technology Investment Plan (2015 Plan). It also provides updates on the acquisition programs and technology initiatives and highlights TSA's recent internal reorganization. This report is best understood as a companion document to the 2015 Plan. The Refresh demonstrates our continuing commitment to transparency with regard to security technology acquisition programs that protect the Nation's aviation transportation systems from terrorist attack. The scope of this Refresh includes the original span of 2016-2020 with additional inputs extending out to 2022.

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

The Honorable Michael McCaul
Chairman, House Committee on Homeland Security

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

The Honorable John Thune
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Bill Nelson
Ranking Member, Senate Committee on Commerce, Science, and Transportation

Inquiries relating to this report may be directed to me at (571) 227-(b)(6) or TSA's Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

David P Pekoske

David P. Pekoske
Administrator

Strategic Five-Year Technology Investment Plan Biennial Refresh

2017 Report to Congress

December 19, 2017

Homeland Security

Transportation Security Administration

Executive Summary

The Transportation Security Administration (TSA) Strategic Five-Year Technology Investment Plan Biennial Refresh aims to achieve a shared vision among congressional, industry, Department of Homeland Security (DHS), and TSA stakeholders to address security technology needs, deploy cutting-edge security capabilities, and increase efficiency and security effectiveness in American aviation security. This report is the first biennial refresh to the original plan, published in August 2015, which was developed in response to the *Transportation Security Acquisition Reform Act of 2014* (P.L. 113-254). This Refresh builds upon updates, and explains alterations to the original plan to provide industry and other stakeholders the most up-to-date sense of the Agency's direction in order to align investments accordingly.

TSA was required to provide an update to the original report and discuss actual acquisitions against planned technology acquisitions from the original report. TSA developed this Refresh in consultation with the DHS Science and Technology Directorate as well as industry stakeholders including the Aviation Security Advisory Committee, Washington Homeland Security Roundtable, and Government Technology and Services Coalition.

The Refresh prioritizes updating information on processes, programs, or initiatives provided in the original report and expanding on those initiatives that have increased in importance for the Agency. As such, this Refresh is a stand-alone document, but certain details may be better understood in the context of the original plan published in 2015 since TSA sought to avoid reporting redundant information.

This Refresh is organized to provide relevant background information, describe TSA's recent agency-wide reorganization and its implications for stakeholders, provide updates to TSA's framework for technology investment based on new policies, delineate the current security technology profile, report on actual technology acquisitions, and discuss technical initiatives and partnerships that will lead to advancing aviation security.

TSA provided substantial updates to information surrounding cybersecurity, the Security Technology Integrated Program, the Innovation Task Force, planned recapitalizations, as well as TSA's methodology for assessing useful life of Transportation Security Equipment (TSE) in response to industry and Congressional feedback on the original report. This Refresh places particular emphasis on the impact of new cybersecurity requirements on TSA's investment plans in light of the Office of Personnel Management hack, which forced TSA to delay deployment of new TSE in order to mitigate cyber threats posed by networking those TSE. A compliance matrix in Appendix G details where requirements from the *Transportation Security Acquisition Reform Act* are fulfilled in the Refresh.

TSA views this Refresh as an important channel to foster dialogue and collaboration with its stakeholders and to provide transparency. TSA looks forward to providing additional updates as mandated by this Act and engaging with stakeholders at industry days and other conferences.

Biennial Strategic Five-Year Technology Investment Plan Refresh

Table of Contents

I. Legislative Language

This document has been compiled to satisfy Section 3 of the *Transportation Security Acquisition Reform Act of 2014* (P.L. 113-245), which amends Section 1611 of the *Homeland Security Act of 2002* (P.L. 107-296). Specifically, this satisfies requirements (g1) and (g2) which state the following:

SEC. 1611. FIVE-YEAR TECHNOLOGY INVESTMENT 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. Background

The Transportation Security Administration (TSA) provides capabilities that drive security across transportation modes and screen all commercial airline passengers and baggage while ensuring the freedom of movement for people and commerce. As presented in the original Strategic Five-Year Technology Investment Plan (2015 Plan), TSA aims to achieve a shared vision among Congressional, industry, and Department of Homeland Security (DHS) stakeholders to increase efficiency and security effectiveness in American aviation security. With this biennial refresh of the 2015 Plan, TSA presents Congress and industry with updates of the aviation security efforts it has initiated, developed, or completed within the last two years. The Refresh extends TSA's commitment to implementing the four themes addressed in the 2015 Plan, which align closely to DHS and TSA strategic policies, as laid out in the *2014 Quadrennial Homeland Security Review* (QHSR). Those themes are:

- Integrating Principles of Risk-Based Security (RBS) in Capabilities, Processes, and Technologies;
- Enhancing Core Mission Delivery by Focusing on a System of Systems;
- Streamlining Acquisitions, Requirements, and Test and Evaluation (T&E) processes; and
- Increasing Transparency in Engagement with Stakeholders to Enable Innovation.

In addition, TSA aims to inform stakeholders of the organizational changes that it has initiated within the last year that will result in an organization that is more efficient, is more transparent, and standardizes the capability definition, development, and deployment process across the Agency. This update will again focus on the aviation security sector, even though TSA has primary responsibility for all modes of transportation except maritime.

In the last two years, TSA's security capabilities have scaled to keep pace with increases in the global commercial aviation industry. TSA continues to operate 365 days a year across roughly 440 airports, and on any given day, TSA and its partners now secure 2.2 million passengers and 1.8 million checked bags on over 25,000 flights – 400,000 more passengers and 600,000 more checked bags, 2 and 5 percent increases respectively, per day than in 2015. Based on Department of Transportation passenger volume forecasts combined with TSA historical and forecasted passenger screening statistics, TSA anticipates that the number of passengers screened will grow by 3 percent in FY 2018. In short, TSA and the aviation industry have seen a steady uptick in daily travelers, and this growth will continue, barring economic downturns. Coupled with ever-evolving threats, the goal for TSA is clear when it comes to technology investment: identify and implement capabilities that can detect increasingly complex threats, secure those capabilities against cyber intrusions, and ensure these capabilities can scale to handle the increasing number of travelers and goods.

A. TSA's Reorganization

Since the release of the 2015 Plan, TSA initiated an Agency-wide reorganization to enhance enterprise leadership of mission support functions, span of control alignment, and acquisition management. The goal for this reorganization is to create a structure that enables enterprise leaders to improve focus on integrating and delivering mission execution and mission support across the full range of TSA's capabilities. TSA recognized the opportunity to enhance its ability to carry out the mission and developed an approach to reorganize at the enterprise and office level. This approach was informed by a variety of stakeholders and assessments, including an independent study by the Defense Acquisition University (DAU).[1]

Primary findings from the DAU study identified a need to create an organizational structure that centralizes acquisition programs in a single chain of command, establishes a dedicated requirements organization to enhance acquisition lifecycle processes, and separates contracting functions from broader acquisition management. Additionally, the study recommended reviewing the location of the Operational Test Agent and deployment and logistics functions. TSA addressed these findings as well as other recommendations through changes at the enterprise and office level.

At the enterprise level, TSA created two new positions below the Administrator level: the Chief of Operations (COO) and the Chief of Mission Support (CMS). The COO works directly with Assistant Administrators (AA) responsible for mission execution to intensify TSA's Agency-wide operational focus and enable TSA to adapt to new threats. The COO serves as the main point of contact for airline COOs and airports, and socializes TSA's unified operational focus to stakeholders. The CMS works directly with AAs responsible for mission support and drives unity of effort and a broad, enterprise approach to human resources, acquisition and procurement, training, logistics, information technology, and other supporting activities.

At the office level, TSA identified opportunities to enhance its acquisition process through internal and external reviews of executive level management and acquisition processes. The results of those reviews prompted TSA to form the Acquisition Reform Task Force (ARTF). The ARTF drafted a phased approach to restructure current acquisition management processes, organizations, and respective personnel. TSA began implementing this approach in December 2016, and at the time of this report, the reorganization is still underway with an expected completion date of December 2017.

The reorganization's first phase realigned the former Office of Acquisition (OA) and Office of Security Capabilities (OSC) into the following three offices:

> ***Office of Requirements and Capabilities Analysis*** **(ORCA)** realigns the legacy OSC requirements and capabilities components into a distinct office. ORCA serves as TSA's Lead Business Authority (LBA) and is responsible for identifying capability needs and determining user requirements. ORCA is also responsible for developing the mission-level requirements in alignment with TSA strategy to support existing and possible future

[1] The Defense Acquisition University is housed within the Department of Defense and provides best-in-class training and perspectives on acquisitions, technology, and logistics.

acquisition programs, starting with conducting capability, human performance, and risk analyses, as well as innovative demonstrations, pilots, and proof of concepts to inform the development of operational requirements. ORCA will coordinate and collaborate with industry and other partners, such as DHS S&T, to identify emerging technologies, perform demonstrations, and develop requirements.

Office of Acquisition Program Management **(OAPM)** will manage all active acquisition programs by end of Calendar Year (CY) 2017, according to TSA's projections. The AA for this office is currently the Deputy Component Acquisition Executive (CAE), and all Program Managers (PMs) that manage DHS Level 1, 2, and 3 acquisition programs either are in this office or will transition into it as the reorganization continues. Also included in this office are Test and Evaluation (T&E), CAE support staff (previously located within the legacy OA) deployment, logistics, and maintenance. Acquisition programs that have achieved Full Operating Capacity (FOC) and transitioned to operational status (or will prior to the end of 2017) will not transition to OAPM. OAPM and the acquisition programs coordinate industry outreach for program maintenance, testing, and other acquisition-related engagement needs. At this time, OAPM manages both the Electronic Baggage Screening Program (EBSP) and Passenger Screening Program (PSP). Additional details and future plans for these programs are included later in the document. OAPM and the acquisition programs coordinate industry outreach for program maintenance, testing, and other acquisition-related engagement needs.

Office of Contracting and Procurement **(OCP)** manages procurement strategy and execution and consists of the legacy OA contracting components. The Head of Contracting Activity (HCA) and contracting specialists are centralized within this office. OCP coordinates industry outreach for contracting actions and opportunities with TSA.

TSA has already made significant changes, but still has several phases to execute until it reaches its desired state. TSA believes that the steps that it has taken to date will result in greater efficiencies, transparency, and harmonization with the development and deployment of capabilities and requirements across the Agency. TSA will provide an update on the reorganization at industry days and in future reports once the next phase is complete. The current enterprise-level organizational chart is provided in Appendix E.

B. Current Strategic Landscape

TSA technology acquisition programs operate within complex environmental realities. As an update to the 2015 Plan, TSA notes the following new considerations:

Evolving and Emerging Threats**:** TSA is subject to an evolving threat environment, and must proactively respond to emerging threats to protect transportation security. The terrorist threat will continue to evolve as terrorists have demonstrated the ability to take advantage of the vulnerabilities in the transportation network around the world.

Evolving Cybersecurity Threats**:** In addition to the exploitation of physical vulnerabilities, TSA must also guard against cybersecurity vulnerabilities. TSA must proactively protect against attacks to steal information or disrupt, destroy, or threaten the delivery of essential services. TSA understands the protection of both the TSE and the underlying network infrastructure against cybersecurity threats, either as part of the initial acquisition or as additional capabilities are applied during upgrades, to be a critical part of its mission.

C. Strategic Priorities and Planning

TSA continues to align its acquisition activities to DHS strategic priorities, including the 2014 QHSR. Furthermore, TSA actively participated in the Department's component roundtables to ensure priorities messaged in this Refresh and the 2015 Plan align to the upcoming QHSR revision. TSA will review the next QHSR, when it is released, to confirm acquisition and other procurement efforts remain in alignment to strategic priorities. Additionally, TSA will continue to evolve its priorities based on the direction of the new Administration and to align with DHS acquisition policy.

As part of its coordination with DHS, TSA continues to collaborate with the DHS Science & Technology Directorate (S&T) to provide high-level strategy for innovative transportation security capability development and enable the successful transfer of technology and/or security solutions.

III. 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. The framework aligns to DHS guidance regarding implementation of the Acquisition Lifecycle Framework (ALF),[2] which outlines key activities for defining, developing, and delivering needed capabilities. In this report, TSA provides specific updates to sections of the Technology Investment Framework.

A. Pre-Need

The Pre-Need phase consists of two analytical phases, both led by ORCA. The first component is the risk assessment process, which continues to assess risk to the transportation sector using intelligence, modeling, and simulation capabilities. The second component in the Pre-Need phase is Capability Analysis. This latter process includes the Transportation Security Capability Analysis Process (TSCAP) that TSA began developing in 2013 to create a structured, repeatable, and transparent requirements generation process. TSA continued to integrate the process and ORCA is responsible for TSCAP under the reorganization. TSCAP can be applied at three levels: holistically across TSA on an annual basis, at the program level to determine requirements for specific gaps, and on a targeted basis in response to specific needs. This report focuses its discussion of TSCAP on the same materiel solution development process discussed in the 2015 Plan.[3]

TSCAP is adapting to align to the new DHS Directive 107-01,[4] which provides the overall policy and structure for Joint Requirements Integration and Management System (JRIMS), set up and governed by the Joint Requirements Council (JRC). DHS uses the JRIMS process to review and validate capability requirements, associated gaps, and proposed mitigation options. This helps to ensure traceability between strategic and capability investments and encourages capability development at the joint or Department level.

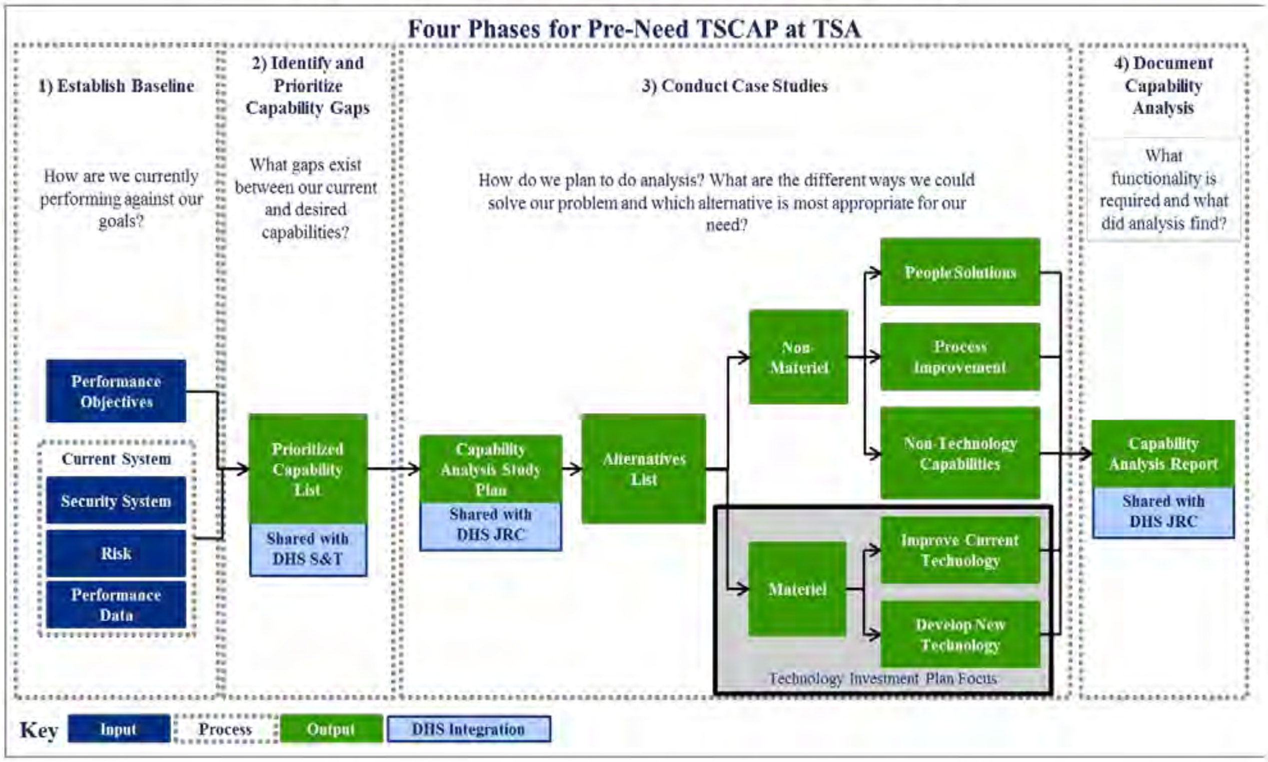
Figure 1 shows the modified TSCAP process. The primary process updates are due to increasing collaboration with DHS in three ways: first, by sharing the prioritized capability list during the Identify and Prioritize Capability Gaps phase; second, by sharing the Capability Analysis Study Plan (CASP) during the Conduct Case Studies phase; and finally by sharing the Capability Analysis Report (CAR) during the Document Capability Analysis phase.

[2] 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).

[3] This references the section beginning on page 8 of the 2015 Plan.

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

Figure 1. Overview of TSA's Capability Analysis Process


Four Phases for Pre-Need TSCAP at TSA
1) Establish Baseline
How are we currently performing against our goals?
2) Identify and Prioritize Capability Gaps
What gaps exist between our current and desired capabilities?
3) Conduct Case Studies
How do we plan to do analysis? What are the different ways we could solve our problem and which alternative is most appropriate for our need?
4) Document Capability Analysis
What functionality is required and what did analysis find?
Performance Objectives
Current System
Security System
Risk
Performance Data
Prioritized Capability List
Shared with DHS S&T
Capability Analysis Study Plan
Shared with DHS JRC
Alternatives List
Non-Materiel
Materiel
People Solutions
Process Improvement
Non-Technology Capabilities
Improve Current Technology
Develop New Technology
Technology Investment Plan Focus
Capability Analysis Report
Shared with DHS JRC
Key
Input
Process
Output
DHS Integration

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.[5] Due to the sensitivity of the prioritized capability gap list, a deprioritized list of the most recent annual capability gap results is provided later in this document. The TSCAP process includes analyzing the capability gaps to identify recommended courses of action (COA) that can further be used to help focus TSA resources on closing critical gaps to an acceptable level. If the only acceptable COA is to implement a materiel solution (i.e., a new device or significant modifications to existing devices), TSA enters the ALF.

B. Acquisition Lifecycle

1. Aligning Resources

The first step, which is a prerequisite for an acquisition, is an analysis of resources to ensure TSA has the correct skill-sets available to support the execution of a potential acquisition or determine how to close any gaps, if necessary. In addition to the steps addressed in the 2015 Plan, TSA now conducts annual acquisition workforce assessments in compliance with DHS Acquisition Program Management Staffing Instructions to maintain consistent visibility into its

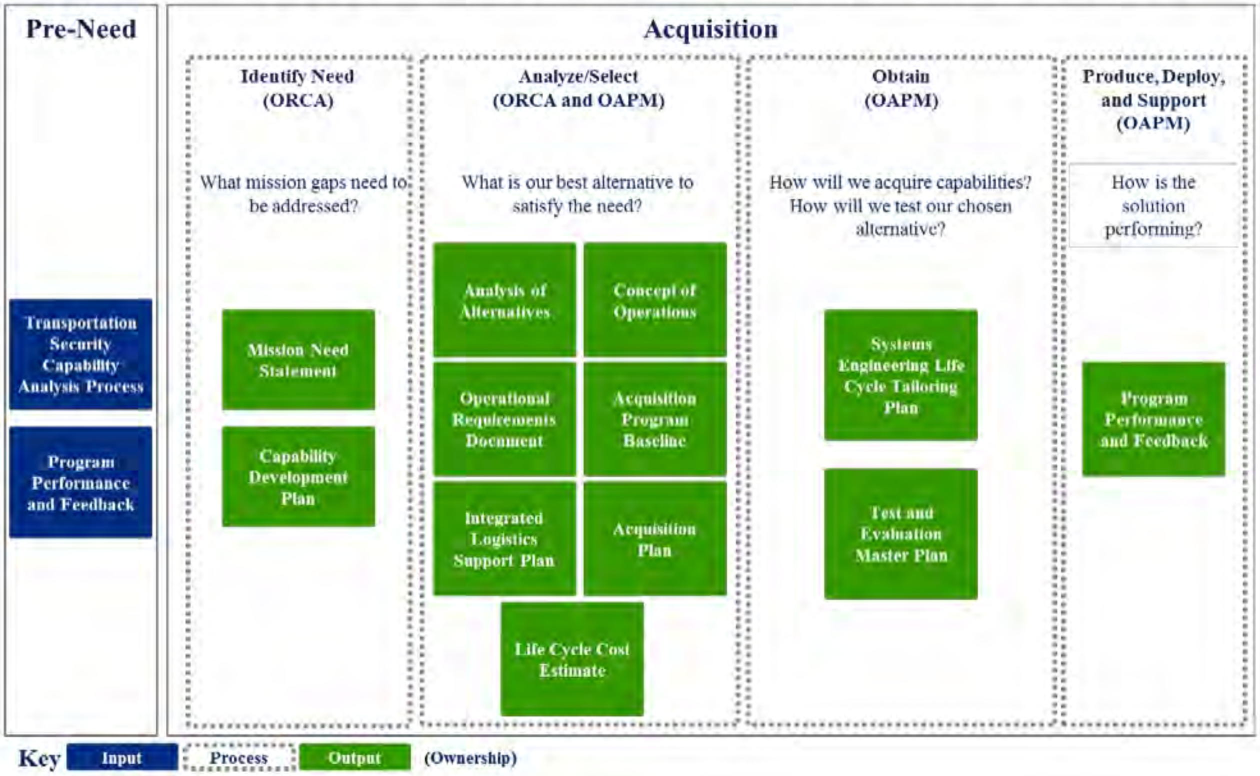
[5] The capability gap prioritization process outlined on pages 8-11 of the 2015 Plan did not require an update and provides additional details on this topic.

workforce needs. Part of this analysis includes a comparison of TSA's staff against DHS's interpretation of Government Accountability Office (GAO) 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 course of 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. CAE is responsible for this step of the acquisition lifecycle.

2. Identifying Needs

TSA transitions from the Pre-Need into the Identifying Needs phase if the Pre-Need COA recommended a materiel solution such as a security-related technology and TSA determined that it had adequate resources to address the gap. As the LBA, ORCA is responsible for using the CARs drafted during the Pre-Need phase to develop the Mission Needs Statement (MNS) and the Capability Development Plan (CDP) with input from applicable programs. Figure 2 depicts the phases of the AD-102 Lifecycle which have formal outputs.

Figure 2. Overview of the Acquisition Lifecycle for Security-Related Technology Materiel Solutions[6]


Pre-Need
Acquisition
Identify Need (ORCA)
Analyze/Select (ORCA and OAPM)
Obtain (OAPM)
Produce, Deploy, and Support (OAPM)
What mission gaps need to be addressed?
What is our best alternative to satisfy the need?
How will we acquire capabilities? How will we test our chosen alternative?
How is the solution performing?
Transportation Security Capability Analysis Process
Program Performance and Feedback
Mission Need Statement
Capability Development Plan
Analysis of Alternatives
Concept of Operations
Operational Requirements Document
Acquisition Program Baseline
Integrated Logistics Support Plan
Acquisition Plan
Life Cycle Cost Estimate
Systems Engineering Life Cycle Tailoring Plan
Test and Evaluation Master Plan
Program Performance and Feedback
Key
Input
Process
Output
(Ownership)

[6] The graphic does not include TSA's processes for 'Aligning Resources' and 'Leveraging Department Efficiencies' as they do not have formal outputs.

3. Analyzing and Selecting Alternatives

The process for analyzing and selecting alternatives remains the same as outlined in the 2015 Plan. ORCA and OAPM are collectively responsible for the documents in this phase and collaborate closely to fulfill these responsibilities.

4. 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, reduce redundancy, drive standardization, streamline procurements, and improve business efficiency.

An example of TSA's use of these vehicles is the Trace Detection (TD) Qualified Products List (QPL), which is the Department-wide ordering vehicle for TDs, which TSA helped develop and manages as the executive agency. Under the TD QPL, TSA solicited to establish a qualified list for the Desktop Explosives Trace Detector (ETD) systems. TSA will continue to leverage this DHS TD QPL strategic sourcing vehicle for future ETD procurements by utilizing the QPL structure to solicit TSA specific requirements and will socialize the list through appropriate channels, such as the Federal Business Opportunities (FBO) website.

DHS also intends to establish strategic sourcing vehicles for both Accessible Property Screening Systems (APSS) and Enhanced Metal Detectors (EMDs) which will be available for TSA to leverage for future procurements. TSA will also be the executive agency for the APSS vehicle.

5. Obtaining Security-Related Technology

TSA has made strides over the past two years to maintain and further the initiatives discussed in the 2015 Plan to accelerate capability delivery and reduce cost.[7] Below, TSA has provided updates for initiatives with significant status changes:

i. Transparency

Testing Documents and Test Plans: TSA understands from industry feedback that the process to share testing documents, plans and the policies to ensure system maturity prior to entering formal testing still lack sufficient transparency. Under the reorganization, OAPM will have the lead for this initiative and will continue to make transparency a priority.

T&E Process Guide: The T&E Process Guide document clarifies policies and responsibilities outlined in DHS Acquisition Management Directive 102 (AD-102) and DHS Management Directive 26-06.[8] TSA is currently updating the T&E Process Guide

[7] This references page 15 of the 2015 Plan.

[8] 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 Testing and Evaluation.

to provide more robust information to industry. The new version of the Process Guide, which is meant to be an external document, will assist industry by:

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

ii. <u>Accelerating Capability Delivery and Reducing Cost</u>

Third Party Testing: OAPM developed a *Third Party Testing* (TPT) Strategy, a sub-function to the QPL process, to outline a plan to reduce the length and cost of the acquisition lifecycle for new systems. OAPM drafted the strategy and received industry feedback through FBO and industry days. Once TSA's T&E Process Guide, referenced above, is finalized, it will supersede the Third Party Testing Strategy. It will provide guidance allowing OEMs to select third party testing organizations and submit these to TSA as part of the QVP submission for TSA's review.

Statistical Methodology: OAPM developed a *Statistical Methodology* Policy to improve the evaluation of test data and increase confidence in the resulting analysis. This policy modifies the evaluation of a system's technical requirements to prevent the likelihood of a significant technical modification being required because of poor performance during Operational Testing (OT) and will use this policy to inform document development.

TSA plans to release an updated TSA T&E Policy, TSA T&E Guidebook, and TSA TPT Strategy to industry within CY 2018.

Additionally, TSA continued to enhance its Qualification Management Plans (QMPs) to streamline requirements development and communication. TSA updated the process by which it will populate QPLs and align with the requirements set forth by DHS within AD-102. This update mapped T&E processes to decision points, and incorporated TPT into the system lifecycle within the requirements release process. The updated process provides review gates and achievable milestones to support contract structures and system readiness to advance within T&E. The first set of requirements to adhere to the new process was the ETD. The changes implemented incorporate DHS Director, Operational Test & Evaluation (OT&E) best practices.

iii. <u>Innovative Concepts</u>

<u>*The Modeling and Simulations Lab*</u>: TSA has created a lab at the TSA Systems Integration Facility (TSIF) called the TSIF Emulation and Simulation Laboratory (TESL) that follows up on the Modeling and Simulation Concept Lab discussed in the 2015 Plan. TESL uses modeling and simulation to explore technological capabilities. This Lab provides space for stakeholders within TSA to collaborate and allows simulations to assess security performance, risk, and human factor components throughout the development and integration lifecycle.

6. Deploying and Supporting Security-Related Technology

TSA continues to deploy and support security-related technology as previously described in the 2015 Plan.[9] Under the reorganization, OAPM is responsible for physical technology deployment.

[9] This references page 16-17 of the 2015 Plan.

IV. Current Security Technology Profile

TSA's current technology profile for aviation security includes approximately 15,000 total deployed TSE across three acquisition programs. TSA identifies, tests, procures, deploys, and maintains equipment that is capable of detecting threats concealed on passengers and in their baggage. EBSP, PSP, and the Security Technology Integrated Program (STIP) are collectively responsible for acquiring new and upgraded technologies to improve aviation security. EBSP procures and supports technology to screen passenger-checked baggage. PSP acquires and supports technology at the passenger screening checkpoint to screen passengers and their carry-on luggage. STIP is an Information Technology (IT) program that works to address the need for the automated exchange of information between TSE and TSA stakeholders. STIP provides for the integration/networking of TSE; this integration/networking increases the degree of effectiveness that TSA and DHS are able to mitigate threats and improve security operations of transportation systems. Additionally, TSA continues to address IT security challenges through cybersecurity initiatives within each program and across the TSE enterprise.

A. Electronic Baggage Screening Program Background

EBSP is a DHS Level 1 acquisition program that supports the TSA mission by testing, acquiring, deploying, integrating, and maintaining technology that screens checked baggage to deter, detect, mitigate, and prevent transportation of explosives or other prohibited items on commercial aircraft, while ensuring freedom of movement for people and commerce.[10]

EBSP measures program performance on an ongoing basis. Metrics are re-evaluated on a regular basis to ensure they adequately represent the effectiveness and efficiency of TSA's program investments. TSA reports relevant metrics to DHS and uses internal targets to assess the health of the program and inform decision-making during program execution. Sample metrics include:

- Maintaining 100 percent screening capability;
- Operational availability of screening technology; and
- Cost per checked bag screened.

The two primary components of checked baggage screening continue to be the Explosives Detection Systems (EDS) and ETD.[11]

B. Passenger Screening Program Background

PSP is a DHS Level 1 acquisition program consisting of multiple technology projects, each at different phases of the acquisition lifecycle. These projects enhance and automate threat detection, further integrate technology and processes, promote a positive passenger experience,

[10] TSA assigns DHS program levels based on AD-102 guidance as prescribed in the current revision for the Acquisition Management Instruction.

[11] This references page 19 in the 2015 Plan.

and enhance collaboration with stakeholders. PSP's goals align to TSA's overarching goals and support TSA's vision to deter and mitigate new and evolving risks by collaborating to quickly field innovative security capabilities. PSP is responsible for identifying, testing, procuring, deploying, and sustaining equipment that detects threats concealed on people and in their carry-on items as they enter the airport terminal sterile area through the passenger screening checkpoint.

PSP measures program performance on an ongoing basis. Metrics are evaluated on a regular basis to ensure they adequately represent the effectiveness and efficiency of TSA's program investments. TSA reports relevant metrics to DHS, and uses internal targets to assess the health of the program and inform decision-making during program execution. Sample metrics include:

- Operational availability for carry-on baggage screening equipment;
- Cost per passenger screened;
- Percent of checkpoint lanes with Advanced Technology (AT) x-rays;
- Percent of checkpoint lanes with Advanced Imaging Technology (AIT); and
- Percent of passengers screened by AIT.

The primary components involved in passenger screening remain the same as in the 2015 report.[12]

C. Security Technology Integrated Program Background

STIP is a program focused on enhancing TSE capability to connect TSE to a network while securing them from cyber threats. TSA has focused more of its efforts on STIP program in response to recent cyber incidents and, as such, is adding it to this report to provide industry with a complete understanding of the program. Historically, STIP focused on achieving the following four goals:

- ***Improve Information Management*****:** STIP collects and disseminates critical data related to TSE, improving situational awareness and risk-based decision-making processes.

- ***Improve Security Agility*****:** STIP enhances TSA's ability to respond to emerging threats by remotely pushing software and other configuration changes to its TSE.

- ***Increase Operational Efficiency*****:** STIP enables TSA to remotely monitor, diagnose, troubleshoot, and manage TSE, allowing TSA to address equipment issues and prevent failures.

Decrease Total Cost of Ownership**:** STIP potentially allows TSA to realize cost benefits as TSE configuration, data collection, and maintenance process are streamlined to reduce on-site visits. To achieve these goals, STIP network connectivity development focused on remediating capability gaps by focusing on improving TSA's performance in the following areas:

[12] This references page 19 in the 2015 Plan.

- **Enterprise Management**
  - Automation of data collection from TSE
  - Automated reports and dashboards that provide holistic views of equipment performance
- **Configuration Management**
  - Accurate verification and tracking of configuration settings (e.g., for Threat Image Projection)
  - Configuration audit of approved baseline to ensure that deployed TSEs are performing per original specifications
- **Resource Management**
  - Automated TSE asset inventory tracking
  - TSE usage tracking
  - Automated tool for Change Control Board (CCB)
- **Equipment Maintenance**
  - Remote diagnostics to streamline maintenance processes
  - Reduced TSE downtime

TSA established STIP as a DHS Level II IT Program to meet these gaps by networking deployed TSE. By June 2015, STIP had networked 2,300 TSE through TSANet (TSA's regular enterprise IT network) and was on track to network 7,000 TSE by the end of CY 2015 and 12,000 by the end of CY 2016.

However, in July of 2015, TSA determined that the networked TSE introduced unacceptable cybersecurity risks to TSANet, especially in light of the enhanced cybersecurity requirements imposed across the government in the aftermath of the Office of Personnel Management (OPM) cybersecurity breach. Consequently, TSA disconnected all TSE and indefinitely postponed all future TSE network connectivity until it could develop and implement appropriate cybersecurity solutions.

TSA is considering options to reconnect the TSE, but resolving this cybersecurity threat is more than just a matter of updating the TSE to the latest operating system patches and reconnecting them to the network. A new solution must address evolving governance and rapidly changing threat environments to be viable and effective. TSA is currently testing solutions to address both the network backend and TSE endpoint cybersecurity risks in order to finalize a comprehensive cybersecurity package to allow TSE to reconnect to STIP. TSA plans to demonstrate a proof of concept to address the TSE endpoint cybersecurity for legacy devices by the end of FY 2018.

D. Planned Technology Programs and Projects Acquisition Update

This section compares security-related technology acquired since 2015 against the planned technology programs and projects in the 2015 Plan per requirement (g2) of the Transportation Security Acquisition Reform Act (TSARA).

TSA operates legacy equipment while evaluating potential replacements in an affordable manner. One way to increase affordability and decrease complete system replacements is the procurement and deployment of technologies to upgrade existing machines as new capabilities arise. Both EBSP and PSP take 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 from the 2015 Plan and other TSA projections did not occur:

- ***897 EMDs in Fiscal Year* (FY) *2016 and 70 EMDs in FY 2017*:** TSA is in the process of qualifying new EMD control heads and anticipates replacing failed legacy components once the process is complete. As a result, TSA does not plan to recapitalize the Walk-Through Metal Detector (WTMD) fleet at this time.

- ***296 ATs 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 these AT units; however, TSA will procure AT units on an "as needed" basis to address airport passenger growth and urgent screening equipment needs.

- ***Credential Authentication Technology (CAT) Units*:** Due to the 2015 cybersecurity breach of the U.S. Office of Personnel Management (OPM), TSA disconnected CAT operational test units in the field until cybersecurity mitigation strategies could be developed and implemented. The determination of cybersecurity mitigations and associated requirements and subsequent development of secure CAT units caused significant schedule delays. Since that time, TSA rebaselined the program and has already been able to place CAT units in four airports for developmental testing and expects to have units in up to 12 airports by the end of CY 2017. TSA now expects to begin fielding CAT units within the next two years.

TSA awarded contracts for the technologies outlined in Figure 3 over the past two years.

Figure 3. TSA TSE Awards, August 2015 – August 2017

TSE	Number Awarded	Timeframe
AIT	161[13]	June 2016, September 2016
AT x-ray	70[14]	September 2015
Boarding Pass Scanner (BPS)	250	August 2016
EDS	115[15]	September 2015, April 2016, August 2016, April 2017
ETD	3426[16]	September 2016

[13] TSA acquired these to provide additional screening capability and for training and testing purposes.

[14] This represents the total units awarded. 15 of these AT x-ray systems were optional systems for the TSA Academy, of which 14 were exercised between September 2015 and May 2017.

[15] TSA acquired these to replace legacy field units and to meet new airport needs based on terminal construction requirements. This figure represents the total units awarded. 18 of these are optional and have not been exercised as of May 2017.

[16] TSA acquired these due to technical obsolescence for a portion of the ETD fleet. This represents the total units awarded. 2,073 of these ETD systems are optional and have not been exercised as of May 2017.

E. Recapitalization and Future Growth

As of September 2016, TSA manages over 15,000 total deployed TSE, across nearly 440 airports.[17] Figure 4 depicts the useful life of currently deployed TSE; the number of TSE deployed as of September 2016 and, more recently, as of May 30, 2017; and the number of airports fielding those TSE.

Figure 4. Overview of Useful Life for Deployed TSE

Currently Deployed TSE	Projected Useful Life	Number Deployed as of 9/30/2016[18]	Number of Deployed as of 5/30/2017	Number of Airports [19]
EDS	15 years	1688	1658	269
ETD *(both EBSP and PSP)*	10 years	5693	5942	433
AIT	10 years	846	876	228
AT	10 years	2199	2170	432
BPS[20]	N/A	2300	2300	421
Bottled Liquid Scanner (BLS)	10 years	1630	1610	425
EMD	10 years	1376	1350	432

The useful life projections outlined in the table above are estimates.[21] TSA replaces TSE at the point of technological obsolescence, which is when TSE cannot be upgraded further to meet new detection standards, but otherwise utilizes the useful life projections provided by original equipment manufacturers (OEMs) or identified in the 2015 Plan as a guide to assess useful life. These projections can change as TSA routinely inspects its deployed technology by analyzing maintenance data, including performance metrics and deployed fleet age information. This reliability, maintainability, and availability data allow TSA to analyze actual performance in the field and re-validate service life estimates annually. TSA also works with industry to identify efficient and innovative ways to extend the life of a TSE. For example, all major components and operating systems of the TSE can now be replaced upon failure, allowing TSE to remain in a high state of readiness without the need for calendar-driven recapitalization efforts.

As mentioned above, TSA monitors TSE detection capabilities and bases recapitalization decisions upon the ability of fielded TSE to respond to changing threats and adhere to new detection standards. TSA plans to replace many of the technologies above with the next generation (Next Gen) equipment outlined below in order to meet new capability needs. TSA continues to recapitalize technologies as needed while new equipment is developed and acquired but otherwise will focus on new program procurements, pending changes to useful life data.

Figure 5 depicts planned purchases for FY 2017 through FY 2020. FY 2017 and FY 2018 data is based on TSA's June 28, 2017 Congressional Spend Plan Briefings for PSP and EBSP. For

[17] 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.

[18] These figures are based on TSA's FY 2016 Congressional Justification.

[19] TSE may also be deployed at additional sites, such as training and test facilities.

[20] BPS data is as of March 2015 due to tracking constraints.

[21] A full discussion of the methodology to arrive at useful life estimates is available on page 21 of the 2015 Plan.

subsequent fiscal years, data is 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 Life Cycle Cost Estimates (LCCEs). The most recently approved LCCEs for EBSP were finalized in July 2015, and for PSP in January 2017. The current cost models will be incorporated in the next LCCEs and TSA will provide those updated figures in the next refresh of this report. These amounts reflect procurements for new systems as well as units being procured to recapitalize existing systems.

To determine long-term budget implications related to operations and support, and in accordance with DHS policy, TSA actively uses LCCEs for its acquisition program to manage cost baselines and balance affordability and requirement trade-offs. The LCCEs that contribute to this report undergo continuous revision as priorities and funding profiles change. Actual purchase quantities are based on available funding and changing realities of the security environment. For example, per Department of Transportation passenger volume forecasts, TSA expects an increase in annual passenger growth, and therefore TSA may look to purchase small quantities of currently qualified systems to respond to airport operations. TSA may also procure evaluation units of new commercial off-the-shelf TSE for demonstrations and developmental testing to assist in the development of future requirements.

Full Operational Capability (FOC) numbers outlined in Figure 5 changed slightly since the last update in 2015. Specifically, the AIT and AT FOC increased since 2015 due to an increase in the number of federalized airports, the number of passengers, and therefore, the number of checkpoints needed.

Figure 5. Approved PSP and EBSP Planned Procurements as of August 2017

TSE	FOC	FY17	FY18	FY19	FY20
EDS[22]	-----[23]	100	190	83	73
ETD *(both EBSP and PSP)*	5860[24]	0	1898[25]	159	10
AIT	962	1	-----	-----	-----
AT	2213	66[26]	-----	-----	-----
BLS	1530	-----	-----	-----	-----
CAT[27]	1520	30	-----	294	295
CT	-----	12[28]	2[29]	2	2
EMD	960	-----	-----	-----	-----
BPS[30]	---	500	-----	-----	-----

[22] EDS planned procurement figures for FY 2017 – FY 2019 are not reflected in the June 28, 2017 Congressional Spend Plan Briefing and program cost models due to an emerging need to recapitalize high-throughput standalone EDS units, as well as deferred projects based on airport schedules.

[23] EBSP met initial FOC in 2003 upon deploying enough ETDs and EDS to screen 100 percent of checked baggage. There are currently 1,670 EDS deployed. Given the improved capabilities of new EDS, such as throughput, and the extended useful life of EDS (currently 15 years), total quantity of deployed EDS fluctuates as operational conditions require.

[24] This is a combined PSP/EBSP ETD count as they are a shared resource. There are 3,222 for PSP and 2,638 for EBSP.

[25] TSA awarded a contract in September 2016 for the purchase of ETDs for the checkpoint, but also included in this award the option to purchase an additional 1,898 ETDs for EBSP. As of August 2017, TSA has chosen not to exercise this option due to technical challenges and anticipates procurement of units in FY 2018.

[26] The procurement of 66 AT units in FY 2017 was not reflected in the June 28, 2017 Congressional Spend Plan Briefing as it is based on a recent, unanticipated need due to federalization of new airports. Based on the PSP Funding Priorities briefed to Congress (Appendix A), money was exercised for this screening equipment (Funding Priority 3) from projects to address capability enhancements, TSA-initiated equipment moves, and airport-initiated equipment moves (Funding Priorities 7, 8, and 9).

[27] The CAT units are not recapitalizations as no units are currently deployed, but they are planned purchases for an existing program. The quantity and fiscal year in which the CAT units are to be purchased are subject to change as the TSA is currently performing developmental testing on the CAT.

[28] TSA reprogrammed funding for initial CT development activities and the procurement, testing, and deployment of 12 CT prototypes.

[29] Two CT units are planned to be purchased under current PSP funding for testing purposes. The two CT units for FY 2019 and FY 2020 reflect a recurrence of money in support of airport expansion.

[30] During development of the 2015 Five-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 APB documentation.

As technology and threats continue to advance, TSA intends to continue to invest in emerging technologies to elevate checkpoint screening capabilities. In early FY 2018, TSA will transition projects currently under PSP to standalone programs to reduce acquisition dependencies and lower overall program risk. These new independent programs are the same as those currently in the PSP program. As expanded capabilities that enhance screening at the checkpoint are introduced, new independent programs will also be implemented. TSA is exploring the following capabilities as potentially independent programs in the future. These are not currently funded programs and, as a result, are not reflected in the previous planned purchase tables.

- Automated Screening Lanes (ASL) will adapt aspects of current baggage handling systems demonstrated by TSA's Innovation Task Force (ITF) to maintain positive bag control at the checkpoint and isolate carry-on bags of interest. The first procurements are anticipated in FY 2020, but if funds are available and there is an identified need, TSA may procure earlier.

- Alarm Resolution devices to resolve identified areas of interest may include Next Gen ETDs or other capabilities. First possible procurements are anticipated in FY 2020.

- Primary Passenger Screening may consist of Next Gen AIT and EMD enhancement and replacement capabilities for performing the primary screening of passengers. First possible procurements are anticipated in FY 2022.

- Accessible Property Screening may consist of Next Gen AT and Computed Tomography (CT). It will consist of devices for performing the primary screening of carry-on baggage. The first procurements for CT are dependent on funding availability and may occur as early as FY 2018.

To meet emerging and evolving threats related to the aviation transportation sector, CT systems offer an enhanced imaging platform as compared to the presently deployed AT x-ray systems and can be upgraded to automatically detect the full range of the APSS detection standard. The APSS detection standard is expected to advance checkpoint capability, as it requires detection of a broader range of homemade explosives, reduced false alarm rates, automated detection for threats and prohibited items, remote image screening, detection of greatly reduced threat mass, and the potential ability for passengers to leave liquids and laptops in bags.

TSA was on a trajectory to invest in CT technology for airport checkpoints with planned purchases of two units in FY 2018 and 2019 for testing purposes and initial deployments under a standalone program in FY 2020. However, in response to emerging threats, TSA is pursuing an incremental acquisition approach, contingent on funding availability.

In FY 2017, Congress approved a reprogramming of $15.3M to fund initial CT development activities and the procurement, testing, and deployment of up to 12 CT prototypes. These prototypes are in addition to the units currently deployed for demonstrations at Logan International Airport and Phoenix Sky Harbor International Airport. TSA will use these prototypes, in the near term, to demonstrate CT systems with capabilities that include enhanced visual interpretation, image manipulation, improved detection of homemade explosives, reduced false alarm rates, and reduced threat mass detection compared to current AT systems.

TSA has drafted an acquisition plan to continue efforts initiated in FY 2017. Under this plan, TSA would rapidly test, procure, and deploy available CT systems via the existing PSP AT x-ray program by FY 2019 and, in parallel, invest in algorithm development efforts to enable CT systems to achieve the APSS detection standard by FY 2019. This approach, the timeline provided below, as well as TSA's deployment strategy are dependent on additional funding resources and the concerted effort from interagency and international partners.

Within FY 2018 TSA intends to procure up to 16 additional prototype CT systems for Operational Assessment (OA) and focus on algorithm development efforts aimed to enable CT systems to achieve the APSS detection standard by FY 2019. The funding requirement to support continued CT development (which includes activities to advance towards the APSS detection standard, operational assessments, and procurement of the 16 additional prototype CT systems) is $35.1M.

In parallel, TSA will accelerate CT acquisition and deployment in the field by qualifying current CT systems under the AT Qualified Products List (QPL). Following successful qualification and operational testing as well as an Acquisition Decision Event, TSA will be able to procure and deploy CT systems to key locations.

The CT quantity need, as defined by the FOC, will be delineated during the Accessible Property Screening program of record acquisition effort, specifically when the Acquisition Program Baseline (APB) and Life Cycle Cost Estimate (LCCE) documents are developed and approved, but based on a complete replacement of AT systems, where feasible, the FOC could potentially be up to 2,279 systems. Ultimately, the number of CT systems to be procured is dependent upon the amount of funding available, the number of CT systems needed to mitigate security risks by airport and by checkpoint, risk, and CT capability. Procurement and deployment decisions will be informed by testing results, operational throughput requirements, and operational procedures.

The anticipated deployment strategy to reach FOC would include procuring and deploying up to 300 systems the first FY. This quantity represents deploying systems to 39 high-risk airports. The funding requirement to deploy 300 systems is approximately $160M, which would support OT&E, procurement, and deployment. As an interim measure, TSA could deploy up to 143 systems to 14 high-risk airports that receive Last Point of Departure (LPD) flights. The funding requirement to deploy 143 systems is approximately $83.5M, which would also support OT&E, procurement, and deployment. In subsequent years, TSA anticipates ramping up the procurement and deployment of systems to a maximum deployment capability of 410 systems per year. To successfully execute this quantity of systems, the full cooperation of airlines, airport authorities, municipalities, and all other key stakeholders is necessary.

As funding is confirmed, TSA will proactively work to keep industry and key stakeholders aware of TSA's latest CT strategy and planned purchases.

Overall, TSA's focus is on meeting capability needs, not on specific technology solutions. That means that these technologies are representative of the technologies TSA will acquire but are not necessarily the exact technologies or quantities TSA will purchase. The information above and in Figure 6 is notional and subject to approved funding. This table is not intended to communicate confirmed planned procurements as these programs may evolve along with the capability areas described above and are shown to provide insight into TSA's strategic direction. Additionally, each of these capabilities must meet TSA and DHS requirements.

Figure 6. New Program Procurement Quantities[31]

Future Programs TSE	FY18	FY19	FY20	FY21	FY22	FY23
ASL	-----	-----	125	125	125	125
Next Gen ETD	-----	-----	8	24	821	819
Next Gen BLS	-----	-----	-----	-----	4	28
Next Gen AIT	-----	-----	-----	-----	4	6
Next Gen EMD	-----	-----	-----	-----	353	352

[31] CAT is not in Figure 6 because those purchases are currently planned under PSP. For the purposes of this plan, please reference the CAT units as shown in Figure 5 to determine future purchase quantities.

F. Cybersecurity

TSA cybersecurity efforts are centralized within the Office of Information Technology and managed by the Chief Information Security Officer. OAPM is responsible for integrating TSA cybersecurity initiatives related to STIP and aviation security technology efforts with acquisition efforts. As TSA continues to move towards a network-connected screening environment through STIP, many IT security challenges need to be addressed proactively to ensure the security of the deployed TSE assets. TSA's current TSE profile includes approximately 15,000 deployed TSE, representing more than 45 different models developed by more than 10 different vendors. The highly customized nature of TSE configuration, coupled with their geographically distributed locations, makes enterprise management difficult from a cybersecurity perspective.

Current challenges to TSE cybersecurity efforts include conducting timely scanning, maintaining compliance with guidelines and standard operating procedures (SOP), mandating IT security requirements for vendors, securing external interfaces, coordinating access control, and securing the physical environments of TSE. TSA has taken steps to identify and implement IT security controls for TSE and position itself for future defense against cybersecurity incidents, including identifying and socializing the cybersecurity capabilities that a TSE would have to meet to connect to TSA's enterprise network.

Moving forward, TSA requires a future state that enables a risk-based cybersecurity regime that is flexible and adaptable to new screening technologies and threats. TSA also needs to comply with mandatory security regulations and DHS policy guidance. This cybersecurity end state for TSA's screening equipment – characterized by a defense-in-depth security architecture, continuous cybersecurity monitoring, and enhanced operational capabilities targeted at maintaining a secure technology environment – must include the following elements:

- Full connectivity of all TSE, enabling two-way data communication;
- Automation of alerts, scans, and patches to comply with Office of Management and Budget (OMB) M-14-03 (November 18, 2013) on continuous diagnostics and mitigation;
- Advanced data encryption standards and access control processes;
- Cybersecurity incorporated into the development and design of future capabilities, instead of being applied retroactively;
- A workforce that understands and supports the importance of cybersecurity and how it enhances mission effectiveness;
- Streamlined cybersecurity configuration management processes; and
- Clearly defined roles, responsibilities, and processes for ongoing and effective collaboration with partners.

To achieve the desired cybersecurity end state, TSA created a comprehensive STIP/TSE cybersecurity plan in 2015 that aims to provide discrete, actionable steps that TSA will take to safeguard the technology, data, and people that its mission supports on a daily basis. DHS's Office of the Inspector General (OIG) acknowledged this plan as a mediating step.

Specifically, this plan:

- Articulates the existing cyber threats and vulnerabilities of TSE to government and industry stakeholders;
- Communicates the goals, activities, and subtasks that mitigate the threats and vulnerabilities;
- Correlates existing capabilities with organizational cyber goals to bring TSA's STIP/TSE environment into compliance with DHS Federal Information Security Management Act (FISMA) cybersecurity and other escalated metrics released by the Federal Chief Information Officer in a cost-effective manner;
- Lays the groundwork for the future acquisition of more secure cyber capabilities; and
- Evolves and adjusts over time to respond to the dynamic nature of cyber threats and new guidance published by the Executive Branch and DHS leadership.

The STIP/TSE cybersecurity plan was also developed based on the STIP/TSE cybersecurity management framework. The framework organizes the lifecycle of security considerations that provides TSA leadership with an adaptable risk-based model to address cybersecurity vulnerabilities. It includes all the elements that encompass processes and procedures to identify and manage cybersecurity risks across technical, operation, and policy fields. The elements include an assessment of the TSE's current cybersecurity posture; establish the desired end state for STIP/TSE cybersecurity; and establish specific goals, activities, and subtasks that the screening equipment programs will implement to close the gaps between current and end-state environments.

TSA's internal cybersecurity frameworks adhere to the standards provided in the publically available DHS 4300A Sensitive Systems Handbook and the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Next Gen TSE will meet the cybersecurity controls outlined in these documents. TSA provides additional information related to these standards to outline where industry can provide assistance through Requests for Information (RFIs).

TSA acknowledges the importance of the cloud as part of cybersecurity initiatives. TSA complies with the Federal Cloud Computing Strategy, and TSA's goal is to harness the power of cloud computing to improve mission effectiveness, improve the security and availability of systems, and protect TSA's data and infrastructure. TSA has fully embraced the Cloud First policy and plans to transition services to the cloud to the greatest extent possible to reduce its data center footprint. Cloud providers will be evaluated based on overall architectural alignment, data security requirements, and cost efficiencies as TSA determines what to move to the cloud, which cloud, and when to transition. TSA OIT has developed a Cloud Computing Security Handbook, which outlines the cloud strategy pertaining to cybersecurity. At the time of this report, TSA expects to publish it in late 2017 and it will be publicly available to federal agencies and industries. This will be a resource for industry and other stakeholders to understand TSA's cloud strategy. TSA continues to update IT policies and procedures as these plans are developed in accordance with the latest TSA IT security plans.

V. Investing in Advancing Aviation Security

TSA continues to make strides in supporting the development of Aviation Security Futures through close coordination with its government partners, industry, and through dedicated internal initiatives. TSA continues to invest in new technology initiatives to meet the evolving threat environment. Specifically, TSA established the Innovation Task Force (ITF) which will be discussed in more detail later in this report. Broadly, in focusing on advancing aviation security, TSA manages solutions across four key dimensions: security effectiveness, operational efficiency, workforce management, and customer satisfaction.

In the last two years, TSA has also invested in the development of a comprehensive system architecture. The continued development and implementation of a system architecture, with an emphasis on open systems, will directly support DHS and TSA resource planning goals and allow ORCA to proactively identify capability gaps and define screening capabilities to address those gaps while also enabling an integrated and modularized security screening system.

A. Technology Capability Gaps

As of 2017, the non-prioritized capability gaps driving technology and investment development 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 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 based on 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; and
- Enhance the ability to adjust security posture based on risk.

TSA has made significant strides towards closing the capability gaps identified through some of the following activities:

> ***Updated Detection Standards*** for AIT, BLS, ETD, checkpoint x-rays and WTMD based on emerging intelligence-based threat streams and actual terrorist events. These updated standards also require a reduction in false alarm rates. Equipment meeting these new standards should provide improved security effectiveness while also providing for improved operational efficiency (i.e., throughput).

Introduced Open System Architecture Elements to increase efficiency and standardization across federalized airports secured by TSA. TSA has begun the development of a system architecture testbed to support architectural requirements validation and capability implementation within an integrated system-of-systems. This testbed can be used to assess requirements for a variety of future capabilities, including common image formats and common graphical user interfaces (GUI) for Next Gen TSE. Through other initiatives such as the Open Threat Assessment Platform (OTAP), TSA is exploring proof of concepts to understand how open architecture TSE prototypes can be used to implement third party detection algorithms, software, and specialized hardware on screening technology. As the organization transitions from focusing primarily on security technologies to holistic requirements and capabilities analysis, an overarching, adaptive, integrated mission architecture can facilitate strategic decision-making. The development of an integrated mission architecture will support TSA's efforts to identify gaps and vulnerabilities, leverage intelligence streams and other information to prioritize the gaps, and help align investments with holistic TSA priorities. Over the next two years, TSA will continue to develop both its system and mission architecture, leveraging lessons learned from the Domestic Nuclear Detection Office (DNDO) Global Nuclear Detection Architecture and efforts of other government entities. ORCA is leading this process and will continue to keep industry informed through a variety of engagement methods, such as industry days and international forums. In the past, TSA has updated industry on progress through a number of forums including the Advanced Development for Security Applications workshop series, the Annual Airport Consultants Council/TSA Security Capabilities Workshop, and other working group meetings.

Automated Prohibited Item Screening to enhance detection capabilities, which can operate without image screeners. Alarms and images will continue to be used by operators to screen for threats. TSA has also been working to develop deep learning capabilities and over the next two years, TSA plans to demonstrate and field deep learning capabilities to augment AT and AIT screening technologies for enhanced security at the checkpoint.

B. Ongoing Technology Initiatives and Innovative Concepts

Below are updates on each of the ongoing technology initiatives and innovative concepts outlined in the 2015 Plan. As mentioned above, ITF is another significant investment by TSA and is a pioneer of innovative concepts. The Enhanced Access to Operational-Like Environments initiative has been removed from this Refresh as the new section on ITF, discussed in a later sub-section, covers this concept.

1. Apex Screening at Speed (SaS*)*

Apex Screening at Speed (Apex SaS), a program led by DHS S&T in collaboration with TSA, was formed to develop solutions for TSA's capability gaps. Apex SaS is pursuing transformative research and development (R&D) activities that support a future vision of a "curb-to-gate" aviation security solution with more effective risk reduction and improved passenger experience. Apex SaS is funding technology development towards a security architecture capable of screening 300 passengers and their carry-on belongings per lane, per hour, at a high detection level with no divestiture of liquids or electronics and dynamic threat adaptation. The technology development efforts under Apex SaS represent short, mid, and long-term investments. For example, walk-by screening at aviation-relevant threats is anticipated to take over five years while efforts such as high-definition CT scanners with augmenting screening capabilities are currently being addressed, with algorithm deliverables anticipated in FY 2018. Apex SaS is working closely with TSA to coordinate technology development to TSA's recapitalization plans as well as ITF to pilot emerging technologies. This coordination will ensure smooth, timely, and effective technology transition from DHS S&T to TSA.

2. Dynamic Aviation Risk Management Solution

TSA's implementation of Dynamic Aviation Risk Management Solution (DARMS), a concept to evaluate flight risk using multiple threat vectors to calculate risk scores on a per-flight basis, has continued to evolve over the past two years as the DARMS Business Case and Concept of Operations (CONOPs) were solidified in 2015. Since that time, TSA completed the architectural design concepts for DARMS and a proof of concept study with DHS S&T. TSA intends to move to a field pilot in the near future and will continue to pursue DARMS as appropriate based on funding. The DARMS concept also takes into account TSA's work with open architecture requirements. TSA will keep industry appraised of progress and will continue to engage with stakeholders to receive feedback.

3. Open Threat Assessment Platform

As previously mentioned, TSA has continued to work on open architecture requirements through its Open Threat Assessment Platform. TSA and Sandia National Labs (SNL) is developing the OTAP, a limited-scope prototype x-ray detection platform that utilizes an open Application Programming Interface, standard data formats, and potentially human-annotated images to aid machine learning and human factors experts in developing algorithms that assist Transportation Security Officers. TSA's continued engagement with the National Labs on the OTAP has the aim of providing a wider variety of vendors with the ability to support capability upgrades across the TSE fleet at lower cost. The desired business outcome is to reward innovation and sustain a healthy vendor market. Ongoing engagement with OTAP has allowed TSA to have the ability to integrate different screening capabilities into a "system of systems" to improve overall screening performance. For example, SNL has collaborated with equipment manufacturers and TSA to demonstrate integration of third-party algorithms with existing TSE. TSA collaboration with OTAP also serves as a tactical step towards dynamic RBS by bridging the gap between TSA and adversary innovation cycles. Future OTAP development, managed in conjunction with DHS S&T, includes demonstration of third-party vendor software integrated with CT x-ray scanners, as well as AIT people screeners.

4. Biometrics

Over the past two years, TSA continued to explore the use of biometrics and began activities to drive forward the strategy for biometric implementation at TSA that will align and compliment DHS' efforts and existing programs to better mitigate the identity validation and vetting risk.

TSA has initiated an operational proof of concept assessment to explore options for improving TSA's ability to verify passenger identity beyond traditional credential authentication measures. In FY 2017, TSA conducted a Biometrics Authentication Technology (BAT) proof of concept using contact and contactless BAT systems at two airports. Following the proof of concept field demonstration, TSA is analyzing the data and will plan for future biometric-based demonstrations considering lessons learned.

Additionally, TSA is coordinating with U.S. Customs and Border Protection (CBP) on applications of biometrics in the operational environment to determine where synergies and opportunities for collaboration may exist, such as the CBP Entry/Exit biometric program for enhanced passenger authentication.

C. Avenues for Innovative Technology Development

TSA continues to work with a number of partners, including government agencies, industry, and academia to develop innovative solutions to solve some of the Nation's toughest security challenges. Specific initiative updates are outlined by stakeholder group below:

1. DHS Science & Technology Directorate

ORCA is primarily responsible for interfacing with DHS Science & Technology Directorate (S&T). Since the 2015 Plan, DHS S&T has continued to provide technical expertise to assist the efforts of TSA. Specifically, the DHS S&T Homeland Security Advanced Research Projects Agency (HSARPA) Explosives Division works to develop innovative, cost-effective systems for screening air cargo, checked baggage, carry-on items, and people at checkpoints that will improve detection capabilities, reduce false alarm rates, and improve the overall customer experience. Additionally, TSA continues to interface and to establish testing priorities and improve testing timelines with the DHS S&T Transportation Security Laboratory (TSL), as well as an additional network of stakeholders through DHS S&T.

2. National Institute of Standards and Technology

Currently, TSA is coordinating with the National Institute of Standards and Technology (NIST) to support the evolution of trace explosive sampling sciences and in-turn, prototype those sampling technologies for TSA-unique requirements to improve sampling and detection capabilities. TSA aims to engage with NIST to conduct a full spectrum of measurement and study activities - both in the laboratory, and in the field – that will support and enhance TSA's capabilities to capture and successfully detect trace levels of explosive threats. For example, several of these efforts include;

- Support training by applying scientifically proven best practices in sample collection;
- Support ETD Analyzer characterization by studying the effects of aging on TSA's ETD fleet;
- Develop Quality Assurance and covert field testing kits and training; and
- Continue to work to enhance TSE interoperability.

3. National Labs

One of the primary vehicles for engagement with the National Labs, the Transportation Systems Analysis Lab Team (TSALT) contract commenced in October 2014 with the vision of providing systems analysis tools and capabilities that can assist in the design and development of a future TSA screening architecture capable of defending against an evolving threat. The TSALT contract is comprised of a consortium of National Laboratories, with SNL being the primary conduit. TSALT is an evolution of the Systems Analysis Working Group partnership that began after the December 2009 Northwest Airlines bombing attempt.

The labs work to achieve TSALT's vision through multiple focus areas to include: adversary characterization, systems architecture, operational effectiveness, and security system solutions. Accomplishments have included the development and operationalization of the Aviation System Security Effectiveness Tool (ASSET), which is the primary tool used in the Risk and Trade Space Portfolio Analyses (RTSPA). Additional achievements include the analysis of threat plotting, analysis of adversary preference for specific threat scenarios using the Adversary Threat Portfolio (ATP), and sourcing of TSE with the goal of cross-cutting vendor platforms.

Looking toward FY 2018 and beyond, the National Labs will continue to focus on adversary characterization efforts and systems architecture support while applying explosive skill-set (ESS) and terrorism skill-set (TSS) expertise to emerging security challenges.

4. University Centers of Excellence

TSA has developed strong partnerships with DHS S&T's University Centers of Excellence (CoE). Close collaboration with two CoEs in particular, the Awareness and Localization of Explosives-Related Threats (ALERT) and the National Consortium for the Study of Terrorism and Responses to Terrorism (START), continues to help TSA refine its explosives analysis and risk analysis processes. TSA representatives participate in government working groups to review CoE research portfolios and ensure mission relevance of each Center's projects. DHS S&T's Office of University Programs involves TSA personnel in competitive selections for new Centers of Excellence. ALERT continues to work with aviation security industry partners on research concepts to assess their feasibility in operational environments. START provides seminars to the TSA workforce to enhance their knowledge of adversarial capabilities, including insider threats. A third CoE, the National Center for Risk and Economic Analysis of Terrorism Events (CREATE), convenes an annual symposium for practitioners and academia. Participants aim to better align research efforts with solutions to transportation security challenges. The University CoEs act as a critical bridge between academic research and technology partners to identify requirements and solutions to aviation security challenges.

5. Partnering with Academia

In addition to University CoEs, TSA seeks to enhance commercial aviation security through partnership with academic institutions. TSA supports academic engineering and technology development activities with equipment manufacturers to ensure the latest science and technology breakthroughs are incorporated in future security systems. Further, TSA frequently hosts science and technology experts to provide seminars in order to maintain technology domain awareness and solicit subject matter expertise in future planning activities.

6. International and Inter-Agency Collaboration and Partnerships

TSA actively pursues inter-agency and international collaboration to enhance commercial aviation security where possible.

For international collaboration, TSA attends ongoing meetings with partners in the European Union (EU), including the European Commercial Aviation Conference (ECAC), to share test and evaluation processes. TSA continues to increase international collaboration with the goal of increasing the worldwide security posture by harmonizing on requirements and sharing best practices and innovative ideas. This includes regular collaboration with the Canadian Air Transport Security Authority (CATSA) and Transport Canada to align efforts on innovation. Additionally, a TSA representative was appointed by Aviation Security (AVSEC) Panel members to be the Co-Rapporteur of the Working Group on Innovation in Aviation Security (WGIAS) of the International Civil Aviation Organization (ICAO). WGIAS consists of scientific, operational, technical, and policy experts to exchange information on initiatives, promote technical awareness, foster collaboration, and act as technical advisors, among other duties.

For inter-agency collaboration, TSA has collaborated closely with CBP to evaluate and implement the use of biometrics where possible, including as a potential method to screen exit lanes from the secure area. Overall, TSA and CBP both have common goals of maintaining/increasing national security while improving the passenger experience.

As previously discussed, TSA also collaborates closely with Federally Funded Research Development Centers (FFRDCs) such as Homeland Security Systems Engineering and Development Institute (HSSEDI) to develop standards and support the development of the System Architecture. Specifically, HSSEDI developed an “As-Is” and “To-Be” architecture as well as an interface and data standards report to inform the development and investment of data and interface standards for the open system architecture. TSA has continued to invest in and socialize the Digital Imaging and Communications in Security (DICOS) Standard, related software library, and conformance testing suite to enable airport security devices to connect over a local area network with a common format for image and metadata. DICOS has gained increasing acceptance as the governing committee developed and released DICOS v2A on May 15, 2017. Additionally, work began on DICOSv3, which will include additional feedback from both OEMs and third party implementers. DICOSv3 will incorporate new modalities and functionalities such as Differential Phase Contrast, Coded Aperture Imaging, and enhancements to the Threat Data Report.

7. Public-Private Partnerships and Small and Disadvantaged Company Participation

In 2016, TSA launched ITF, a public-private partnership with industry and transportation security system stakeholders to demonstrate emerging capabilities in transportation security environments. The ITF has mobilized stakeholders across the aviation ecosystem to demonstrate solutions. For the ASL demonstration, airport authorities, air carriers, and vendors contributed funding to support the successful demonstration. ITF actively works to engage with small businesses in order to support development of new and innovative solutions. TSA will continue to support small businesses to generate innovation in security.

8. Innovation Task Force

<u>Background:</u>

ITF supports TSA in diversifying the industrial base while responding to industry and stakeholder requests to increase access to operational data to mature solutions and provide input on future transportation security capabilities. TSA formed ITF in part due to industry feedback and discussions during the creation of the initial 2015 Plan. Following the reorganization, ITF is now under ORCA. Through ITF, TSA is developing both a strategic and tactical approach to demonstrate innovative and holistic solutions within operational airports to address the threat landscape, improve the passenger screening experience, and deliver the concept of reservation-to-destination screening capability.

Solutions may cover a breadth of concepts, from aesthetic design changes to new detection technologies, supporting near-term and long-term progress towards the future TSA system architecture. ITF demonstrates selected innovative and systemic solutions to improve effectiveness, posture for future passenger growth, and evolve to deter and detect an adaptive enemy. It enables TSA and industry to refine potential emerging transportation security capabilities and requirements. Demonstrations of innovative, emerging capabilities increase access to operational environments for stakeholders to help provide real-life operational experience to reduce technology transition time and cost, and better inform TSA requirements.

As TSA develops its mission architecture over the next two years, a key focus will be to better understand current performance of the security technology portfolio and to generate initiatives to prototype, pilot, and implement solutions. These efforts will diagnose current performance across three key dimensions: security effectiveness, operational efficiency, and customer experience. Key themes from the strategy highlight several major needs, which the ITF will seek to address through solutions:

- Expand resources beyond standard screening spaces to counter emerging threats while improving effectiveness;
- Increase agility and flexibility of workforce management systems, including better predictive tools and better data to improve front-line workforce engagement;
- Improve operational consistency and efficiency to maintain security effectiveness and improve customer satisfaction; and

- Better coordinate across stakeholders to improve the quality and pace of fact-based decision making.

ITF Demonstration Processes:

Standard processes are used to evaluate and establish sites, select near- and long-term solutions, and inform future requirements and decisions. ITF selects sites using a site selection methodology, including a standard criteria and approach. Once a site is selected, it moves through the site lifecycle, which covers the key phases and steps from site set-up and solution selection and installation through closeout of each event and site. Following closeout, the resulting analyses and lessons learned are documented and provided to the appropriate office, program, or organization for consideration in requirements development, solution development, or acquisition planning.

ITF Solutions and Project Areas:

Since standup in 2016, the first ITF operational demonstration was initiated for ASLs, and subsequently to multiple airports around the country via an Urgent Operational Need (UON). This demonstrated ITF's ability to capture lessons learned to inform requirements. Outside of ASLs, ITF has also identified additional solutions for demonstration and expanded the pool of interested partners. Several recently initiated or upcoming solution demonstrations for ITF are:

- CT demonstrations with three different manufacturers;
- Initial BAT PoC demonstrations;
- Passenger communication tools as TSA and airports identify tools and techniques for checkpoint enhancements; and
- Enhanced AIT demonstrations as they are available.

In addition to solution demonstrations, ITF will also collaborate with airlines, airports, and industry partners to facilitate innovation through projects such as:

- Information Technology and Operations Collaboration: pilot an Airport Operations Center (AOC);
- Large Mass Threat Detection: pilot portable mass casualty focused employee and public area screening with potential for high throughput and reduced divestiture; and
- Biometric Bag Drop: pilot a self-checked bag drop solution with biometric validation of identity by airlines.

Another focus for ITF is the Innovative Demonstrations for Enterprise Advancement (IDEA) process. The goal for IDEA is to encourage the development of diverse, forward-looking solutions to increase the probability of achieving enhanced, comprehensive security solutions. IDEA allows TSA to improve its understanding of existing market capabilities and identify vendors capable of enhancing the transportation security system.

For stakeholder engagement, ITF also has an Industry Exchange (iX) strategy. This strategy allows ITF to customize activities for different industry events based on expected audience, type of event, and intended outcome. ITF has established and is in the process of refining an iX toolkit composed of concepts that "inform stakeholders" and "pulse the market."

One example of these events was a "shark tank" style quick pitch at AAAE's annual conference where vendors had the opportunity to explain their solution and go through a mock evaluation process and obtain user feedback directly from an STSO. Industry expressed positive feedback about the effort and a number of solution submissions were directly tied to this engagement at AAAE.

In order to successfully demonstrate solutions, ITF must identify partners in airports, airlines, and other federal agencies. By targeting exchange efforts to answer industry's questions, ITF will have more informed stakeholders and greater industry knowledge making future broad Agency announcements and solution demonstrations go more smoothly. ITF intends to use these events to collaborate with industry and spread awareness of future solicitations, identify solutions for demonstration, and enhance industry's understanding of TSA's requirements and needs.

ITF's Role in TSA Acquisitions:

ITF aligns with the future TSA vision for systems architecture and does not replace TSA offices' current responsibilities and efforts to advance aviation security. ITF operates in alignment to DHS AD-102, which establishes solution demonstrators, as well as in alignment to the Acquisition Lifecycle Framework, as depicted below in Appendix F.

ITF demonstrations provide data on new, future-focused solutions, which is then used as an input for the Pre-Need phase, as outlined earlier in this report. ITF also provides partners with demonstration data to improve and refine solutions, reducing the time needed to refine a solution, and inform documentation. This may enhance the rapid acquisition of capability to deliver Next Gen security effectiveness and operational efficiency.

Ultimately, ITF demonstrations are considered successful if TSA gains an enhanced understanding of a challenge and receives operational efficiency and security effective data on a solution as a result of the demonstration.

VI. Conclusion

TSA developed this Strategic Five-Year Technology Investment Plan Biennial Refresh to provide a status update to TSA's stakeholders, to include Congress, DHS, industry, and others, taking into consideration several environmental factors such as cybersecurity, an internal reorganization of the Agency, and the transition of a new Administration. TSA is constantly seeking to improve its processes to better serve the traveling public and to coordinate with industry, as seen with the organizational changes and new initiatives TSA has implemented within the last two years.

Appendices

A. Program Priorities

This appendix explains program-funding priorities in addition to TSE purchase needs. The recapitalization numbers and Next Gen procurement figures outline the TSE that TSA is planning to purchase, but these priority lists explain how funds are otherwise used to support program operations on an on-going basis. In supporting this mission, the Program prioritizes funding by first focusing on its core functions.

Passenger Screening Program Priorities

Mission critical priorities include:

1. Critical Program Operations Management: Includes staffing, training, and other critical costs required to execute the program(s).

2. System Maintenance: Sustainment of TSE after deployment. Examples include:
   a. Safety requirements to properly and effectively operate equipment.
   b. Post Implementation Reviews (PIRs) to validate systems are meeting requirements, investment goals are being achieved, and lessons learned are being captured.
   c. Sustainment activities do not include system upgrades/enhancements.

3. Screening Equipment: Procurement and deployment of checkpoint TSE and associated ancillary equipment needed for airport operations. This does not include deployment of screening equipment in support of non-TSA special events. Examples include:
   a. Airport expansions
   b. New federalized airports
   c. Training facilities

4. Emerging Threats: Urgent projects to quickly address new threats and vulnerabilities. An example would be the development and deployment of solutions.

5. Planned Threat Detection Enhancements: Development of planned, incremental enhancements in support of threat detection capabilities. Such capabilities can be achieved through currently deployed TSE software and/or hardware field upgrades. This does not include deployment of the enhancements.

6. Recapitalization of Equipment: Upgrade or replacement of TSE that have reached their end of useful life based on technical obsolescence and other program drivers (such as reliability, availability, or maintainability). This includes deployment of planned threat detection enhancements.

After mission-critical projects have been funded, PSP considers investments in projects that will increase checkpoint efficiencies:

7. TSE Capability Enhancements: Development and deployment of TSE system-level enhancements in support of operational efficiencies. This only includes TSE-specific capability enhancements (such as Common GUI improvements, workstation modifications, and non-detection related software changes).

8. TSA-Initiated Equipment Moves: Movement of checkpoint screening equipment in support of TSA-initiated activities. This does not include deployment of screening equipment in support of non-TSA special events.

9. Airport-Initiated Equipment Moves: Movement of checkpoint screening equipment in support of airport-initiated activities.

This funding prioritization is reviewed as part of TSA's Planning, Programming, Budgeting, and Execution (PPBE) process to address updates to operational priorities and constraints.

Electronic Baggage Screening Program Priorities

1. Program Operations and Management: Managing the program and appropriate staffing, training, equipment testing and other support costs.

2. Equipment to Ensure 100 percent Screening Compliance: Procuring and deploying TSE to maintain 100 percent screening compliance.

3. Critical Operational Projects: Executing unforeseen and urgent projects to quickly remedy unacceptable safety issues or security vulnerabilities.

4. Fulfillment of Existing Obligations: Fulfilling projects with executed letters of intent or other transactional agreements. Also purchasing and installing equipment required for those projects.

5. Threat Detection Capability Development: Developing threat detection algorithms, but does not include the deployment of these capabilities.

6. System-Level Capability and Operational Efficiencies: Developing and deploying EDS system improvements to increase EDS lifespan, create efficiencies, and decrease alarm rates.

7. Recapitalization or Upgrade of Equipment Due for Useful Life Replacement: Replacing or upgrading aging machines that have reached the end of useful life, deploying new threat detection algorithms and risk-based security (RBS) capabilities, and upgrading network equipment in support of capability enhancements.

Limited funding available:

8. Airport-Level Capability and Operational Efficiencies: Installing new in-line systems and implementing improvements to facilitate compliance.

9. Reimbursement of Systems Completed without a TSA Funding Agreement: Reimbursing airport operators who had a reasonable expectation of reimbursement for costs incurred while developing or deploying in-line systems in the absence of a funding agreement.

EBSP prioritizes competitive procurement for EDS, using competitive bidding by qualified vendors to determine the EDS OEM for checked baggage screening projects, allows the program to tailor the requirements for the EDS OEM to each individual project. TSA evaluates planned EDS projects throughout the year to determine both the schedule for EDS procurements and the opportunities that may exist for a given project to be competed between qualified vendors. This competition determination is done as early as possible in the planning/design phase of a project and is made based on specific factors unique to each individual project.

B. Stakeholder Engagement Activities

TSA engaged industry and government stakeholders in the creation of this report. TSA recognizes the importance of its industry and government partners and solicited input and feedback throughout the development of the Refresh.

TSA: Internal stakeholders within the TSA participated in the creation of the Plan with the intent of collecting knowledge from each office and division and aligning vision for the Plan through review and feedback sessions. Engaged teams included the ORCA, OAPM, OIT, OCP, Office of Security Operations (OSO), Office of the Chief of Performance and Enterprise Risk (CPER), and Office of Finance and Administration (OFA). The scope of this engagement included working sessions, meeting, and virtual input requests.

The Department of Homeland Security and Other Government Agencies: DHS S&T were engaged with the intent of coordinating and collaborating with counterparts to inform the Plan's strategic and technological components.

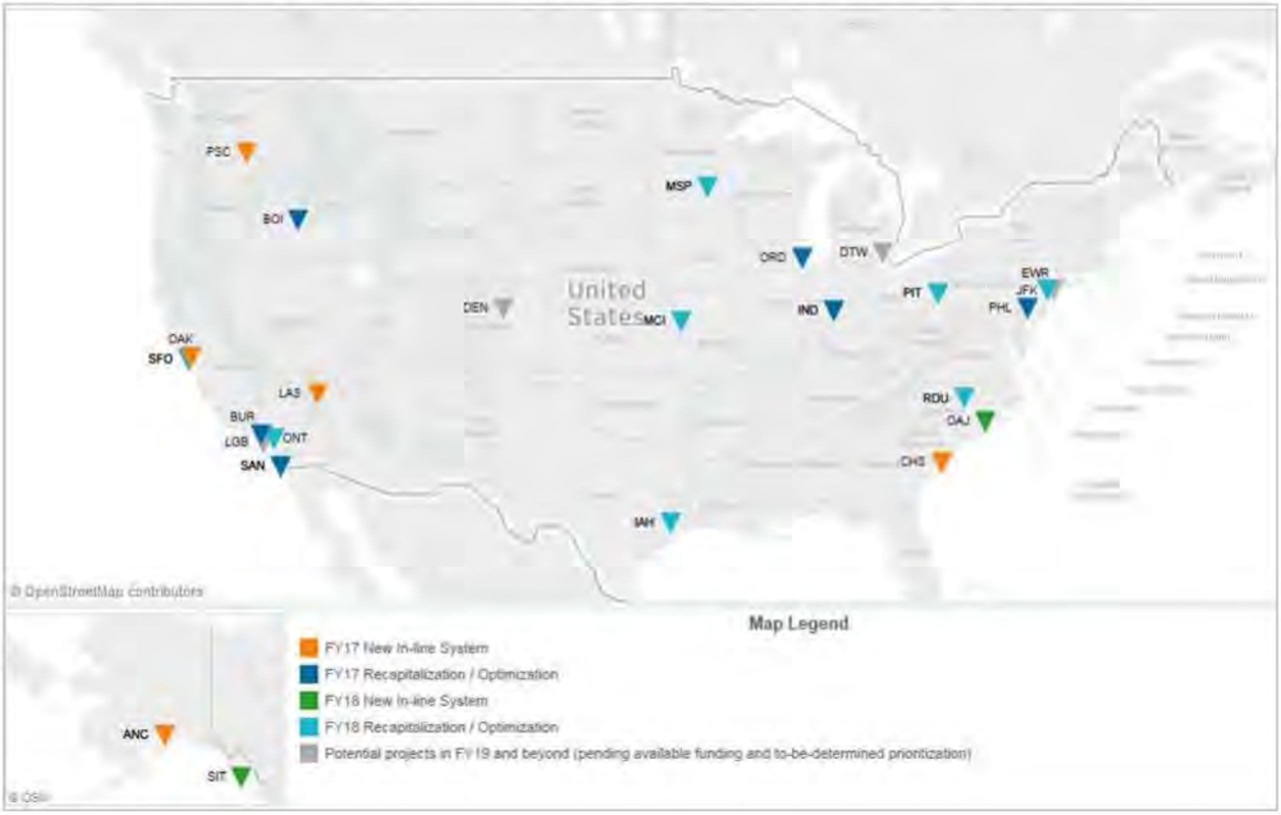
Industry: TSA provided a draft copy of the report for review and comment to the Aviation Security Advisory Committee (ASAC), Washington Home Security Roundtable (WHSR), and the Government Technology and Services Coalition (GTSC). These groups represent a significant portion of TSA's stakeholders. Additionally, GTSC represents small and mid-sized industry organizations, and is a new group TSA engaged this year.

Comments were collected from members of these groups and addressed where possible based on the scope of the report. All other comments were documented, and TSA may address them in future reports or in future industry days.

C. Airport Other Transactional Agreement List

TSA strives to ensure checked baggage screening zones utilize screening equipment capable of meeting the existing baggage demand in the most operationally efficient manner. To support this, TSA has had an average other transactional agreement (OTA) spend of $192 million dollars from FY 2012 to FY 2016. Figure 7 details the location of planned checked baggage inspection system projects for FY 2017 and FY 2018, including recapitalization and optimization projects, as well as proposed airport projects beyond FY 2019. Final planning for airport projects is ongoing, and projects will be considered according to the strength of their contribution toward fulfilling the Agency's mission to protect the Nation's transportation systems. This preliminary information is provided for contextual awareness, and changes to this information should be anticipated.

Figure 7. Planned or Proposed EDS Projects: FY 2017 – FY 2019


PSC
BOI
MSP
ORD
DTW
United States
DEN
MCI
IND
PIT
EWR
JFK
PHL
OAK
SFO
LAS
BUR
LGB
ONT
SAN
RDU
OAJ
CHS
IAH
© OpenStreetMap contributors
ANC
SIT
© OSM
Map Legend
🟧 FY17 New In-line System
🟦 FY17 Recapitalization / Optimization
🟩 FY18 New In-line System
🟦 FY18 Recapitalization / Optimization
⬜ Potential projects in FY19 and beyond (pending available funding and to-be-determined prioritization)

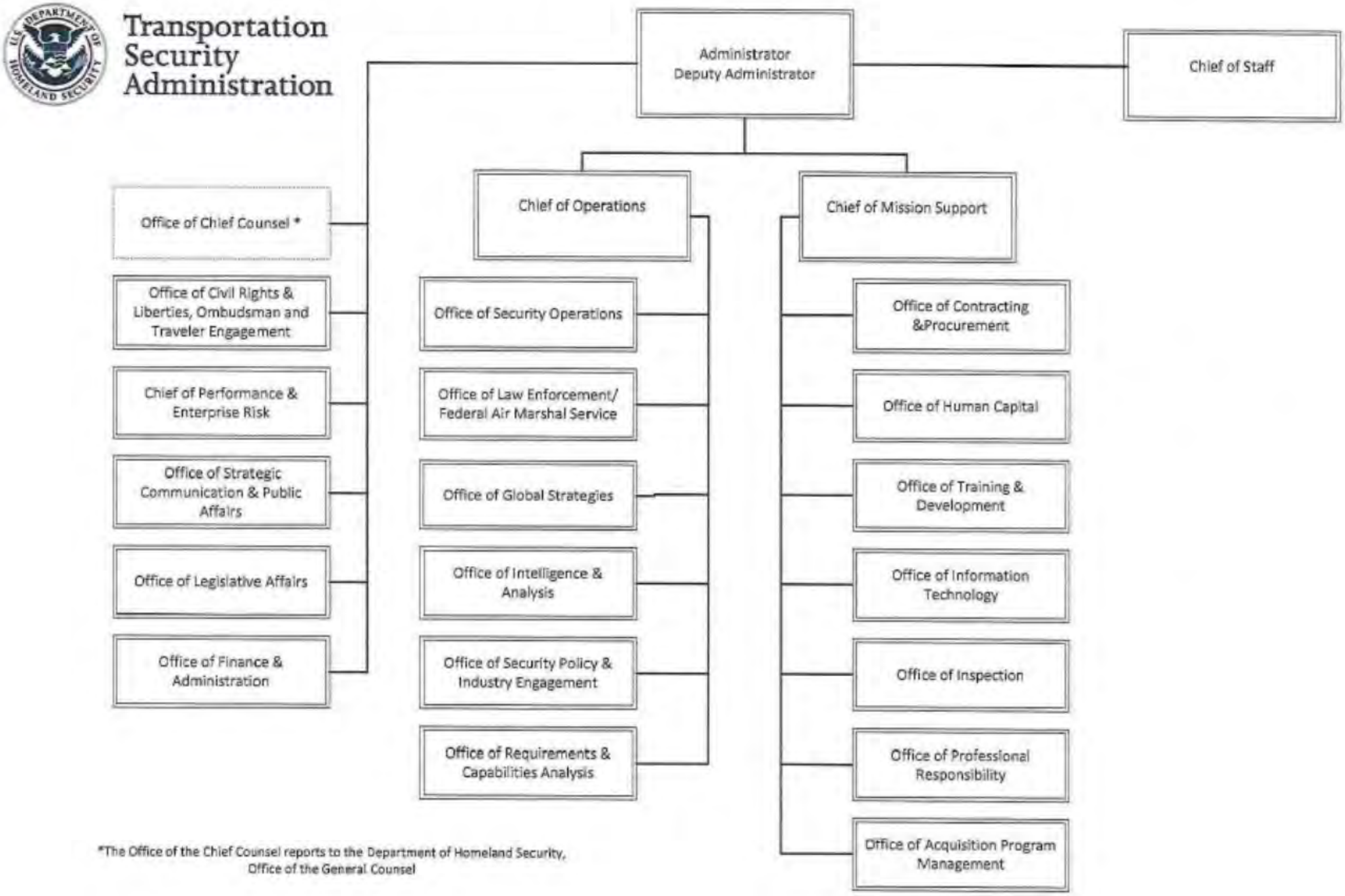
D. Acronym Table

Acronym	Phrase
AA	Assistant Administrator
AIT	Advanced Imaging Technology
ALERT	Awareness and Localization of Explosives-Related Threats
ALF	Acquisition Lifecycle Framework
ANL	Argonne National Lab
AOC	Airport Operations Center
APSS	Accessible Property Screening System
ARP	Alarm Resolution Program
ARTF	Acquisition Reform Task Force
ASAC	Aviation Security Advisory Committee
ASL	Automated Screening Lane
ASSET	Aviation System Security Effectiveness Tool
AT	Advanced Technology
ATP	Adversary Threat Portfolio
AVSEC	Aviation Security
BAT	Biometrics Authentication Technology
BLS	Bottled Liquid Scanner
BPS	Boarding Pass Scanner
CAE	Component Acquisition Executive
CAR	Capability Analysis Report
CASP	Capability Analysis Study Plan
CAT	Credential Authentication Technology
CATSA	Canadian Air Transport Security Authority
CBP	U.S. Customs and Border Protection
CCB	Change Control Board
CDP	Capability Development Plan
CMS	Chief of Mission Support
COA	Course of Action
CoE	Center of Excellence
CONOPs	Concept of Operations
COO	Chief of Operations
CPER	Chief of Performance and Enterprise Risk
CSS	Checkpoint Strategy Simulator
CT	Computed Tomography
CY	Calendar Year
DARMS	Dynamic Aviation Risk Management Solution
DAU	Defense Acquisition University
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office (DNDO)

Acronym	Phrase
EBSP	Electronic Baggage Screening Program
ECAC	European Commercial Aviation Conference
EDS	Explosives Detection System
EMD	Enhanced Metal Detector
ESS	Explosive Skill-Set
ETD	Explosives Trace Detector
EU	European Union
FAA	Federal Aviation Administration
FBO	Federal Business Opportunities
FFRDC	Federally Funded Research Development Centers
FISMA	Federal Information Security Management Act
FOC	Full Operational Capability
FY	Fiscal Year
GAO	Government Accountability Office
GTSC	Government Technology and Services Coalition
GUI	Graphical User Interface
HCA	Head of Contract Activity
HSARPA	Homeland Security Advanced Research Projects Agency
HSSEDI	Homeland Security Systems Engineering and Development Institute
ICAO	International Civil Aviation Organization
IDEA	Innovative Demonstrations for Enterprise Advancement
INL	Idaho National Lab
IT	Information Technology
ITF	Innovation Task Force
iX	Industry Exchange (iX)
JRC	Joint Requirements Council
JRIMS	Joint Requirements Integration and Management System
LBA	Lead Business Authority
LCCE	Lifecycle Cost Estimate
MNS	Mission Need Statement
Next Gen	Next Generation
NIST	National Institute of Standards and Technology
OA	Office of Acquisition
OAPM	Office of Acquisition Program Management
OCP	Office of Contracting and Procurement
OEMs	Original Equipment Manufacturers
OFA	Office of Finance and Administration
OPM	Office of Personnel Management
ORCA	Office of Requirements and Capabilities Analysis
OSC	Office of Security Capabilities
OSO	Office of Security Operations

Acronym	Phrase
OT	Operational Testing
OTA	Other Transactional Agreement
OTAP	Open Threat Assessment Platform
PIR	Post-Implementation Review
PM	Program Manager
PoD	Plan of Day
PPBE	Planning, Programming, Budgeting, and Execution
PPS	Primary Passenger Screening
PSP	Passenger Screening Program
QHSR	Quadrennial Homeland Security Review
QMP	Qualification Management Plan
QPL	Qualified Products List
R&D	Research and Development
RBS	Risk-Based Security
RFI	Request for Information
RTSPA	Risk and Trade Space Portfolio Analyses
S&T	Science & Technology
SaS	Screening at Speed
SAWG	Systems Analysis Working Group
SNL	Sandia National Labs
SOP	Standard Operating Procedure
START	Study of Terrorism and Responses to Terrorism
STIP	Security Technology Integrated Program
TD	Trace Detection
T&E	Test and Evaluation
TPT	Third Party Testing
TSA	Transportation Security Administration
TSALT	Transportation Systems Analysis Lab Team
TSARA	Transportation Security Acquisition Reform Act
TSCAP	Transportation Security Capability Analysis Process
TSE	Transportation Security Equipment
TSIF	Transportation Security Administration Systems Integration Facility
TSL	Transportation Security Laboratory
TSS	Terrorism Skill-Set
UON	Urgent Operational Need
WGIAS	Working Group on Innovation in Aviation Security
WHSR	Washington Home Security Roundtable
WTMD	Walk-Through Metal Detector

E. TSA Reorganization – Organizational Chart



Transportation Security Administration

Administrator
Deputy Administrator

Chief of Staff

Office of Chief Counsel *

Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement

Chief of Performance & Enterprise Risk

Office of Strategic Communication & Public Affairs

Office of Legislative Affairs

Office of Finance & Administration

Chief of Operations

Office of Security Operations

Office of Law Enforcement/ Federal Air Marshal Service

Office of Global Strategies

Office of Intelligence & Analysis

Office of Security Policy & Industry Engagement

Office of Requirements & Capabilities Analysis

Chief of Mission Support

Office of Contracting &Procurement

Office of Human Capital

Office of Training & Development

Office of Information Technology

Office of Inspection

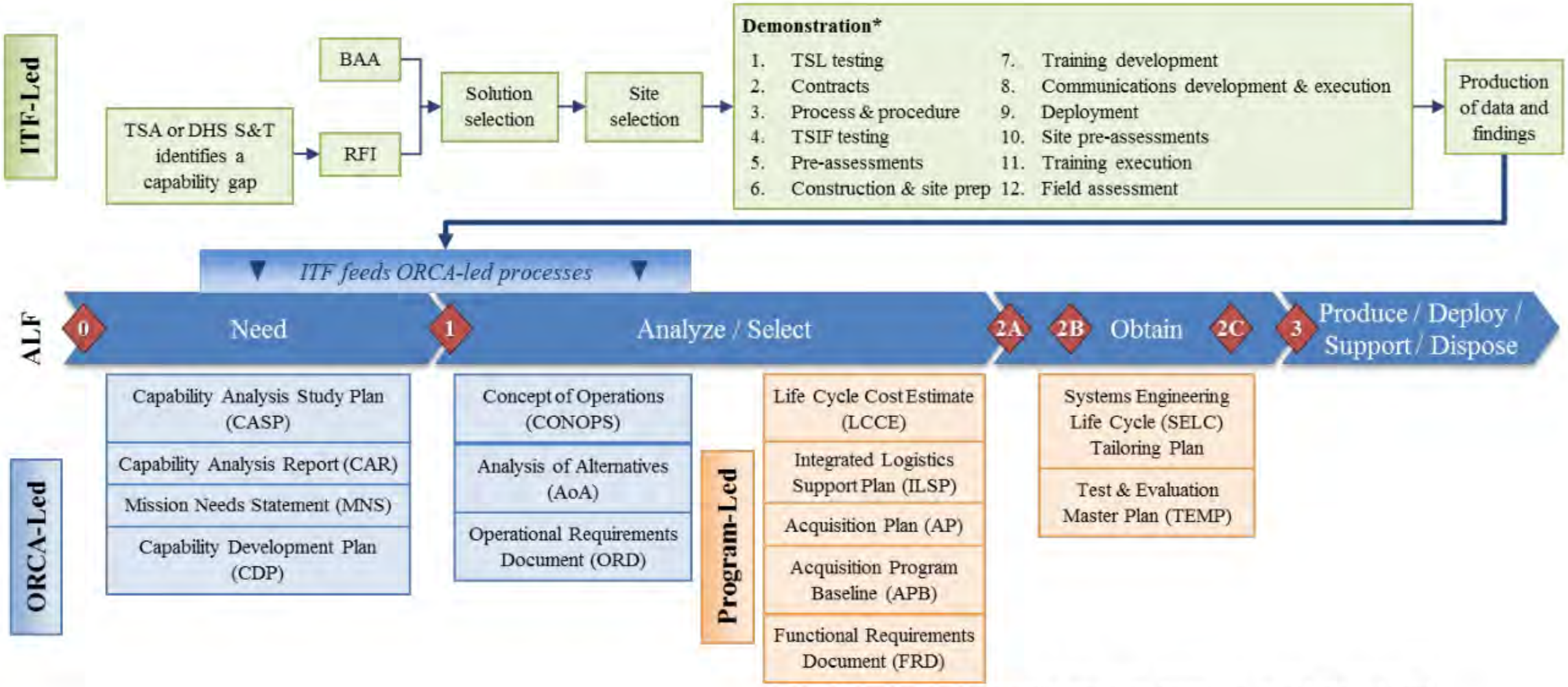
Office of Professional Responsibility

Office of Acquisition Program Management

*The Office of the Chief Counsel reports to the Department of Homeland Security, Office of the General Counsel

F. Innovation Task Force in the Acquisition Lifecycle Framework

Appendix F depicts the role of ITF in the Acquisition Lifecycle, which aligns to Figure 2 in the Technology Investment Framework.



ITF-Led
TSA or DHS S&T identifies a capability gap
BAA
RFI
Solution selection
Site selection
Demonstration*
1. TSL testing
2. Contracts
3. Process & procedure
4. TSIF testing
5. Pre-assessments
6. Construction & site prep
7. Training development
8. Communications development & execution
9. Deployment
10. Site pre-assessments
11. Training execution
12. Field assessment
Production of data and findings
ITF feeds ORCA-led processes
ALF
0
Need
1
Analyze / Select
2A
2B
Obtain
2C
3
Produce / Deploy / Support / Dispose
ORCA-Led
Capability Analysis Study Plan (CASP)
Capability Analysis Report (CAR)
Mission Needs Statement (MNS)
Capability Development Plan (CDP)
Concept of Operations (CONOPS)
Analysis of Alternatives (AoA)
Operational Requirements Document (ORD)
Program-Led
Life Cycle Cost Estimate (LCCE)
Integrated Logistics Support Plan (ILSP)
Acquisition Plan (AP)
Acquisition Program Baseline (APB)
Functional Requirements Document (FRD)
Systems Engineering Life Cycle (SELC) Tailoring Plan
Test & Evaluation Master Plan (TEMP)

* Note: Demonstration activities may vary depending on solution selected

G. 2017 Five-Year Plan Refresh – Compliance Matrix

TSA's intent for the 2017 Refresh is to meet the g(1) and g(2) requirements to update the 2015 Plan. TSA is providing this compliance matrix to show which of the original requirements were discussed in the Refresh and where that discussion occurred.

Table 1: Five-Year Plan Refresh Compliance Matrix

Requirement	Requirement Description	Report Location	Pages
b(1)	Develop Five-year technology investment plan in consultation with Under Secretary for Management.	*Not Required for Refresh*	
b(2)	Develop Five-year technology investment plan in consultation with Under Secretary for Science and Technology.	*Not Required for Refresh*	
b(3)	Develop Five-year technology investment plan in consultation with the Chief Information Officer.	*Not Required for Refresh*	
b(4)	Develop Five-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.	*Investing in Advancing Aviation Security –* Technology Capability Gaps	19
d(1)	The plan shall include consideration of the most recent Quadrennial Homeland Security Review (QHSR).	*TSA Background –* Current Strategic Landscape	6
d(2); d(2)A	The plan shall include a set of security-related technology acquisition needs, prioritized based on risks and associated capability gaps.	*Investing in Advancing Aviation Security –* Technology Capability Gaps *Current Security Technology Profile -* Program Profiles	19 11 - 13

Requirement	Requirement Description	Report Location	Pages
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.	*Current Security Technology Profile –* Program Profiles *Investing in Advancing Aviation Security –* Ongoing Technology Initiatives and Innovative Concepts	11 - 13 20 -21
d(3)	The plan shall include an analysis of current and forecasted trends in domestic and international passenger travel.	*TSA Background*	4
d(4)	The plan shall include an identification of currently deployed security-related technologies that are at or near the end of their life-cycles.	*Current Security Technology Profile –* Recapitalization Numbers	14
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	*Technology Investment Framework –* Technology Investment Framework	7
d(6)	The plan shall include identification of opportunities for public-private partnerships.	*Investing in Advancing Aviation Security –* Avenues for Innovative Technology Development	23 – 24
d(6)	The plan shall include identification of opportunities for small and disadvantaged company participation.	*Investing in Advancing Aviation Security –* Avenues for Innovative Technology Development	23 – 24
d(6)	The plan shall include identification of opportunities for intra-government collaboration.	*Investing in Advancing Aviation Security –* Avenues for Innovative Technology Development	23

Requirement	Requirement Description	Report Location	Pages
d(6)	The plan shall include identification of opportunities for university centers of excellence.	*Investing in Advancing Aviation Security* – Avenues for Innovative Technology Development	22 – 23
d(6)	The plan shall include identification of opportunities for national laboratory technology transfer.	*Investing in Advancing Aviation Security* – Avenues for Innovative Technology Development	22
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.	*Technology Investment Framework* – Aligning the Workforce	8
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.	*Current Security Technology Profile* – Cybersecurity	17 – 19
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.	*Technology Investment Framework* – Acquisition Lifecycle	8 – 11
d(10)	The plan shall include an impact assessment to commercial aviation passengers.	*Technology Investment Framework* – Pre-Need	7 – 8
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.	*Technology Investment Framework* – Acquisition Lifecycle – Deploying and Supporting Security Related Technology	11

Requirement	Requirement Description	Report Location	Pages
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.	*Investing in Advancing Aviation Security –* Technology Capability Gaps	19
e(1)	To the extent possible, and in a manner that is consistent with fair and equitable practices, the plan shall leverage emerging technology trends and research and development investment trends within the public and private sector.	*Investing in Advancing Aviation Security*	19 – 26
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.	*Appendix B: Stakeholder Engagement Activities*	*29*
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.	*Current Security Technology Profile –* Program Profiles	11 – 13
f	With the 5-yr technology-investment plan, a list of non-government persons that contributed to the writing of the plan shall be provided.	*Not Required for Refresh*	
g(1)	Beginning two 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.	*The Refresh*	1 – 40
g(2)	Beginning two 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.	*Current State* – Planned Technology Programs and Projects Acquisition Update	13 - 14

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598-6028

Transportation
Security
Administration

ACTION

MEMORANDUM FOR: David P. Pekoske
Administrator

THROUGH: Patricia F.S. Cogswell 7/19/2018
Patricia F.S. Cogswell
Deputy Administrator

Stacey Fitzmaurice /s/
Executive Assistant Administrator
Operations Support

FROM: Austin J. Gould /s/
Assistant Administrator
Requirements and Capabilities Analysis

SUBJECT: Approval of TSA Biometrics Roadmap

Purpose

To request your approval of the Transportation Security Administration (TSA) Biometrics Roadmap for Aviation Security and the Passenger Experience.

Background

In April 2018, the TSA front office requested the Assistant Administrator of Requirements and Capabilities Analysis (RCA) to develop a biometrics roadmap for your signature by the end of June 2018. RCA last updated you on the roadmap during the pre-brief for the U.S. Customs and Border Protection (CBP)/TSA Senior Guidance Team meeting on June 18, 2018.

From April to June, RCA had more than 40 targeted engagements with strategic aviation security leaders from airlines, airports, and solution providers. RCA also met with CBP and the U.S. Department of Homeland Security Office of Biometric Identity Management to obtain feedback on the roadmap. TSA's Policy Coordination Branch coordinated concurrences from Assistant Administrators whose offices are affected by this roadmap.

Discussion

Identity verification is a cornerstone of TSA's operational landscape in the commercial aviation sector. In order to meet the challenges of evolving security threats, rising air travel volumes, resource constraints, and limits on operational footprint, TSA and aviation security regulators around the globe must look to automate manual and paper-based identity verification processes through smart technology investments.

The TSA Biometrics Roadmap lays out a practical approach to leveraging biometric technologies to improve security effectiveness and operational efficiency while also enhancing the passenger experience. Your approval of this roadmap positions RCA to communicate TSA's approach to biometrics with industry partners, including airports, airlines, and technology companies.

TSA is stepping into the biometric solution space at an ideal time to capitalize on technological advancements in biometric system accuracy, speed, and ability to automate high-throughput operations. Additionally, travelers are increasingly amenable to biometric technologies and the enhanced security and efficiency they can provide. Publishing this roadmap is an important step in accelerating TSA's growth in the aviation security biometric landscape.

Recommendation

Recommend you approve and sign the TSA Biometrics Roadmap. RCA will use the roadmap to socialize TSA's approach for biometrics with airline, airport, and technology partners.

Approve David P Pekoske ______ Date
5 Aug 2018

Disapprove ______________________ Date

Modify ______________________ Date

Needs more discussion ________________ Date

Page 01

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25

Withheld pursuant to exemption

(b)(6) ; (b)(5)

of the Freedom of Information and Privacy Act

Page 26

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 27

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 36

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 37

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 38

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 39

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 48

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 49

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 68

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

U.S. Department of Homeland Security
Freedom of Information Act Branch
601 South 12th Street
Arlington, VA 20598-6020

Transportation
Security
Administration

August 27, 2020

3600.1
Case Number: 2020-TSFO-00198

Ashley Gorski
Patrick Toomey
Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
agorski@aclu.org
nspfoia@aclu.org

Dear Ms. Gorski:

This is the Transportation Security Administration's (TSA) second interim response to your Freedom of Information Act (FOIA) request dated January 09, 2020, addressed to the TSA FOIA Branch seeking access to "records pertaining to the use of facial recognition technology at airports and at the border by the Department of Homeland Security ('DHS'), U.S. Customs and Border Protection ('CBP'), and the Transportation Security Administration ('TSA')." That request seeks the following records from TSA:

1. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning:

> *a. The acquisition, processing, retention, or dissemination of data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
>
> *b. Access by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities to data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
>
> *c. Retention or dissemination by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities of data collected or generated through CBP's biometric services and infrastructure, including biometric templates.*

2. All final evaluations, tests, audits, analyses, studies, or assessments by the DHS Science and Technology Directorate, DHS Office of Biometric Identity Management, or the National Institute of Standards and Technology related to (i) the performance of algorithms in matching facial photographs, and/or (ii) the performance of facial recognition technologies developed by vendors. This request encompasses records concerning whether the algorithms or technologies perform differently based on flight route or an individual's race, ethnicity, skin pigmentation, gender, age, and/or country of origin.

3. All records, excluding informal email correspondence, concerning future interoperability between the TSA's biometric capabilities and "mission partner systems," including CBP and DHS Office of Biometric Identity Management systems.

4. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate information-sharing. [Note that we understand that in May 2020 the ACLU agreed to rephrase this request as follows: 'All policies, procedures and guidelines concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate biometric information-sharing.']

5. All records, excluding informal email correspondence, concerning the TSA's plans to "complement the capabilities" of Credential Authentication Technology through the implementation of TVS or facial recognition technology with respect to domestic travelers.

6. All records, excluding informal email correspondence, concerning whether implementation of biometric technologies would result in operational efficiencies, including whether, at certain airport facilities, "the throughput of the checkpoint may be largely unaffected" by biometric technology because "a faster [travel document checker] process would merely shift traveler volume from the queue into the screening lane."

The processing of TSA's second interim response identified certain records that will be released to you. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552. Please refer to the Applicable Exemptions list at the end of this letter that identifies the authority for withholding the exempt records by marking the block next to the applicable exemptions. An additional enclosure with this letter explains these exemptions in more detail.

For this second interim response, the TSA FOIA Branch reviewed 753 pages, of which we have released in full 211 pages, released in part (with redactions) 14 pages, withheld in full 72 pages, identified 9 pages as duplicates and 2 pages as non-responsive. Additionally, we sent 16 pages to CBP for consultation, and sent 9 pages to DHS for consultation.

We processed an additional 420 pages, which we have determined are publicly available on line at the following links:

- https://doi.org/10.6028/NIST.IR.8238
- https://www.tsa.gov/sites/default/files/foia-readingroom/final_2018_nsts_signed.pdf
- https://www.dhs.gov/sites/default/files/publications/TSA%20-%20Advanced%20Integrated%20Passenger%20and%20Baggage%20Screening%20Technologies_0.pdf
- https://www.commerce.senate.gov/2019/9/protecting-the-nation-s-transportation-systems-oversight-of-the-transportation-security-administration

The rules and regulations of the Transportation Security Administration applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 6, Part 5. They are published in the Federal Register and are available for inspection by the public.

Administrative Appeal

Because TSA’s response to this request is currently the subject of litigation, the administrative appeal rights normally associated with a FOIA request response are not being provided.

If you have any questions pertaining to your request, please contact AUSA Jennifer Jude at jennifer.jude@usdoj.gov.

Sincerely,

Teri M. Miller
FOIA Officer

Summary:
Number of Pages Released in Part or in Full: 225
Number of Pages Withheld in Full: 72

APPLICABLE EXEMPTIONS
FREEDOM OF INFORMATION ACT AND/OR PRIVACY ACT

Freedom of Information Act (5 U.S.C. 552)

☐ (b)(1) ☐ (b)(2) ☐ (b)(3) ☐ (b)(4) ☒ (b)(5) ☒ (b)(6)

☐ (b)(7)(A) ☐ (b)(7)(B) ☐ (b)(7)(C) ☐ (b)(7)(D) ☐ (b)(7)(E) ☐ (b)(7)(F)

Enclosures

FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Transportation Security Administration (TSA) FOIA Branch applies FOIA exemptions to protect:

Exemptions

Exemption (b)(1): Records that contain information that is classified for national security purposes.

Exemption (b)(2): Records that are related solely to the internal personnel rules and practices of an agency.

Exemption (b)(3): Records specifically exempted from disclosure by Title 49 U.S.C. Section 114(r), which exempts from disclosure Sensitive Security Information (SSI) that "would be detrimental to the security of transportation" if disclosed.

Exemption (b)(4): Records that contain trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

Exemption (b)(5): Inter- or intra-agency records that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege:

- Deliberative process privilege – Under the deliberative process privilege, disclosure of these records would injure the quality of future agency decisions by discouraging the open and frank policy discussions between subordinates and superiors.
- Attorney work-product privilege – Records prepared by or at the direction of a TSA attorney.
- Attorney-client privilege – Records of communications between an attorney and his/her client relating to a matter for which the client has sought legal advice, as well as facts divulged by client to attorney and any opinions given by attorney based on these.

Exemption (b)(6): Records that contain identifying information that applies to a particular individual when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." This requires the balancing of the public's right to disclosure against the individual's right to privacy.

Exemption (b)(7)(A): Records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information…could reasonably be expected to interfere with law enforcement proceedings.

Exemption (b)(7)(C): Records containing law enforcement information when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy" based upon the traditional recognition of strong privacy interests ordinarily appropriated in law enforcement records.

Exemption (b)(7)(E): Records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Exemption (b)(7)(F): Records containing law enforcement information about a person, in that disclosure of information about him or her could reasonably be expected to endanger his or her life or physical safety.

PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

Transportation Security Administration (TSA) FOIA Branch applies Privacy Act exemptions to protect:

<u>Exemptions</u>

Exemption (d)(5): Information compiled in reasonable anticipation of civil action or proceeding; self-executing exemption.
Exemption (j)(2): Principal function criminal law enforcement agency records compiled during course of criminal law enforcement proceeding.
Exemption (k)(1): classified information under an Executive Order in the interest of national defense or foreign policy.
Exemption (k)(2): Non-criminal law enforcement records; criminal law enforcement records compiled by non-principal function criminal law enforcement agency; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.
Exemption (k)(5): Investigatory material used only to determine suitability, eligibility, or qualifications for federal civilian employment or access to classified information when the material comes from confidential sources.
Exemption (k)(6): Testing or examination material used to determine appointment or promotion of federal employees when disclosure would compromise the objectivity or fairness of the process.