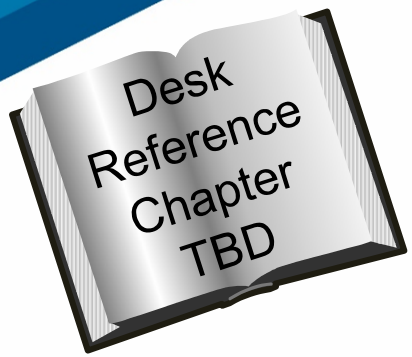


AAAE Basics of Airport Law Workshop
TSA Legal Update
Chicago, Illinois

Francine J. Kerner
TSA Chief Counsel
October 9, 2024

TSA Mission, Vision, and Core Values

MISSION

Protect the nation's transportation systems to ensure freedom of movement for people and commerce.

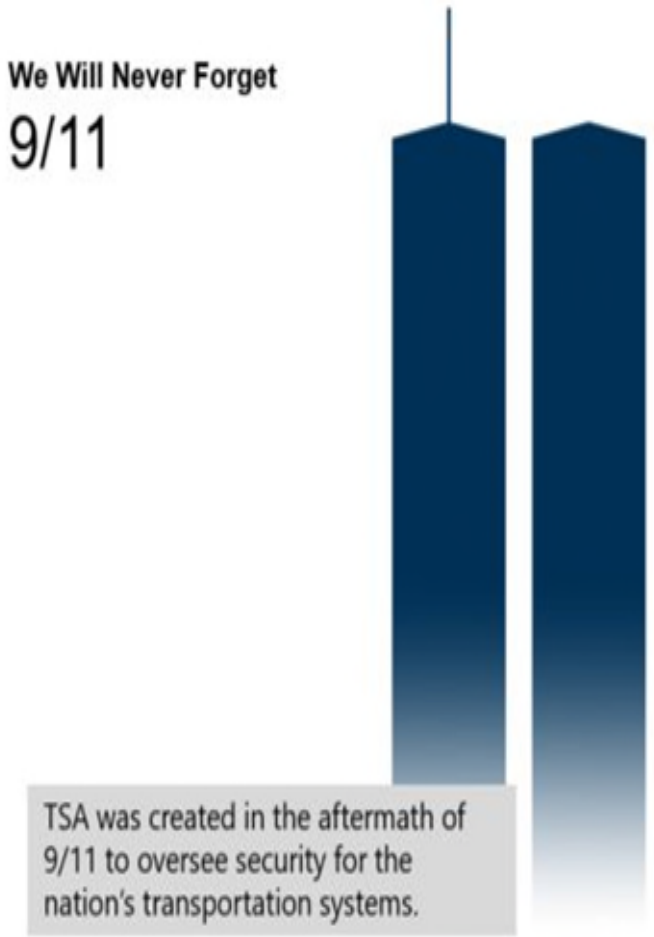
VISION

An agile security agency, embodied by a professional workforce, that engages its partners and the American people to outmatch a dynamic threat.

CORE VALUES

Integrity. Respect. Commitment.

Our Establishing Years



2001

President George W. Bush signed the Aviation & Transportation Security Act.

2002

Federalization of security operations was finished by the end of 2002.

2003

TSA officially became part of the Department of Homeland Security.

Evolution of Threats to Aviation

1970 - 1980s

Hijackings for hostages using guns, knives, and grenades.

Threat
Hiding bombs in electronics, attacks on the public side of airports, and insider threats.

Responses
Enhanced Accessible Property Screening, Public Area Security Summit, review flight school vetting, accelerating deployment of Computed Tomography.

Threat
Hijackings not for hostages but using planes as weapons; bombs using unique methods of concealment (shoes, underwear, soft drinks).

Responses
Advanced Imaging Technology, liquids ban, improved ID verification, using intelligence to identify higher risk passengers for enhanced screening.

Threat
The COVID-19 Pandemic presented a novel public health threat to the traveling public; increased cybersecurity threats to aviation and critical infrastructure; and specific, identified threats to cargo.

Responses
Mask mandate, travel restrictions, and changes to the TSA checkpoints. Cybersecurity requirements in Security Programs and recommendations in Information Circulars. Heightened requirements for certain types of shipments from specific countries.

Let's Talk Numbers…

- 4 million miles of roadways
- 140,000 miles of railroad tracks
- Approximately 615,000 bridges and 526 roadway tunnels
- 3.3 million miles of pipeline

TSA's top ten busiest travel days have occurred since May 2024

3,000 outbound international flights & 23,000 domestic flights DAILY.

+/- 34m

CREDENTIAL HOLDERS VETTED EACH **MONTH,** NOT INCLUDING PASSENGERS VETTED BY SECURE FLIGHT

5.5m

CARRY-ON ITEMS SCREENED DAILY

1.4m

CHECKED ITEMS SCREENED DAILY

2.3m

PASSENGERS SCREENED DAILY

Select TSA Authorities

Aviation and Transportation Security Act (ATSA), P.L. 107-71 (Nov. 19, 2001).	➢ TSA's Mission: Oversee security in all modes of transportation regulated by DOT ➢ Includes TSA's emergency powers
National Emergencies – 49 U.S.C. 114(g)	➢ During a national emergency, TSA Administrator responsible for coordinating all domestic transportation, including "transportation-related responsibilities of other departments and agencies"
Regulatory Authority – 49 U.S.C. 114; 40113; 44932	➢ Outlines TSA Administrator's responsibilities ➢ Provides authority to conduct investigations, prescribe regulations, standards, and procedures, and issue orders. ➢ Provides authority to ensure adequacy of airport security measures
Security Directives and Information Circulars – 49 CFR 1542.303	➢ Provides a regulatory standard for issuing SDs and ICs when TSA determines that additional airport security measures are necessary to respond to a threat
Screening – 49 U.S.C. 44901	➢ TSA "shall provide for the screening of all passengers and property" ➢ Screening "shall be carried out by a Federal Government employee"

Select TSA Authorities

Airport Security Program – 49 U.S.C. 44903(c)	➢ Airport operators are required to maintain an air transportation security program and must provide "a law enforcement presence and capability" that "is adequate to ensure the safety of passengers"
TSA Amendments to Airport Security Programs – 49 CFR 1542.105	➢ Allows TSA to amend a security program based on safety and the public interest; sets forth procedures for amendment
Background Checks – 49 U.S.C. 114(f)(12)	➢ Requires background checks for personnel with access to secure areas of the airport (ex. SIDA badge)
Secured Area and Perimeter Access – 49 U.S.C. 44903(g)-(h)	➢ TSA is charged with the regulation of secured area access control and airport perimeter access security
Foreign Airport Security – 49 U.S.C. 114; 44907	➢ TSA assesses security measures maintained at foreign airports with flights to the United States.
Federal Air Marshal Service (FAMS) – 49 U.S.C. 44917	➢ Air Carriers are required to provide seating on any flight to a FAM

Select TSA Authorities

Cybersecurity Authority – 49 U.S.C. 44912(b)	➢ Requires TSA to "review threats to civil aviation, with particular focus on…the disruption of civil aviation service, including by cyber attack"
Cybersecurity Authority – 49 U.S.C. 114 note (TSA Modernization Act § 1989(d))	➢ The Administrator shall manage TSA's cybersecurity risks, evaluate the cybersecurity of TSA's trusted traveler and credentialing programs and remediate as needed, and upon request conduct cybersecurity vulnerability assessments for airports and air carriers.
Visible Intermodal Prevention and Response (VIPR) Teams – 6 U.S.C. 1112	➢ TSA Administrator may develop VIPR teams "to augment the security of any mode of transportation at any location"

Sensitive Security Information (SSI) Protection and Handling

SSI is information that, if publicly released, would be detrimental to transportation security. 49 CFR part 1520	
SSI Requirements	Lock Up all SSI: Store SSI in a secure container, such as a locked file cabinet or drawer. Destroy SSI When No Longer Needed: Destruction of SSI must be complete, to preclude recognition or reconstruction of the information. Mark SSI: Even when only a small portion of a document contains SSI, every page of the document must be marked as SSI.
Covered Persons	Only covered persons, such as Airport and Aircraft operators and Indirect Air Carriers, are authorized to access SSI.
Requests for SSI	Refer to TSA for guidance to ensure proper protection of SSI.
Unauthorized Disclosure of SSI	Report to TSA or applicable agency.
Examples	Airport Security Programs, vulnerability assessments, and cybersecurity documents.

Our Guiding Documents

DAVID PEKOSKE
ADMINISTRATOR

ADMINISTRATOR'S INTENT (AI)

AI 3.0 was released in July 2023

Airport Related Objectives include: Advanced Air Mobility, Threat Detection, and Insider Threats

CAPITAL INVESTMENT PLAN

Budget related document forecasting future investments in screening technology

STRATEGIC PRIORITIES & PLANNING GUIDANCE

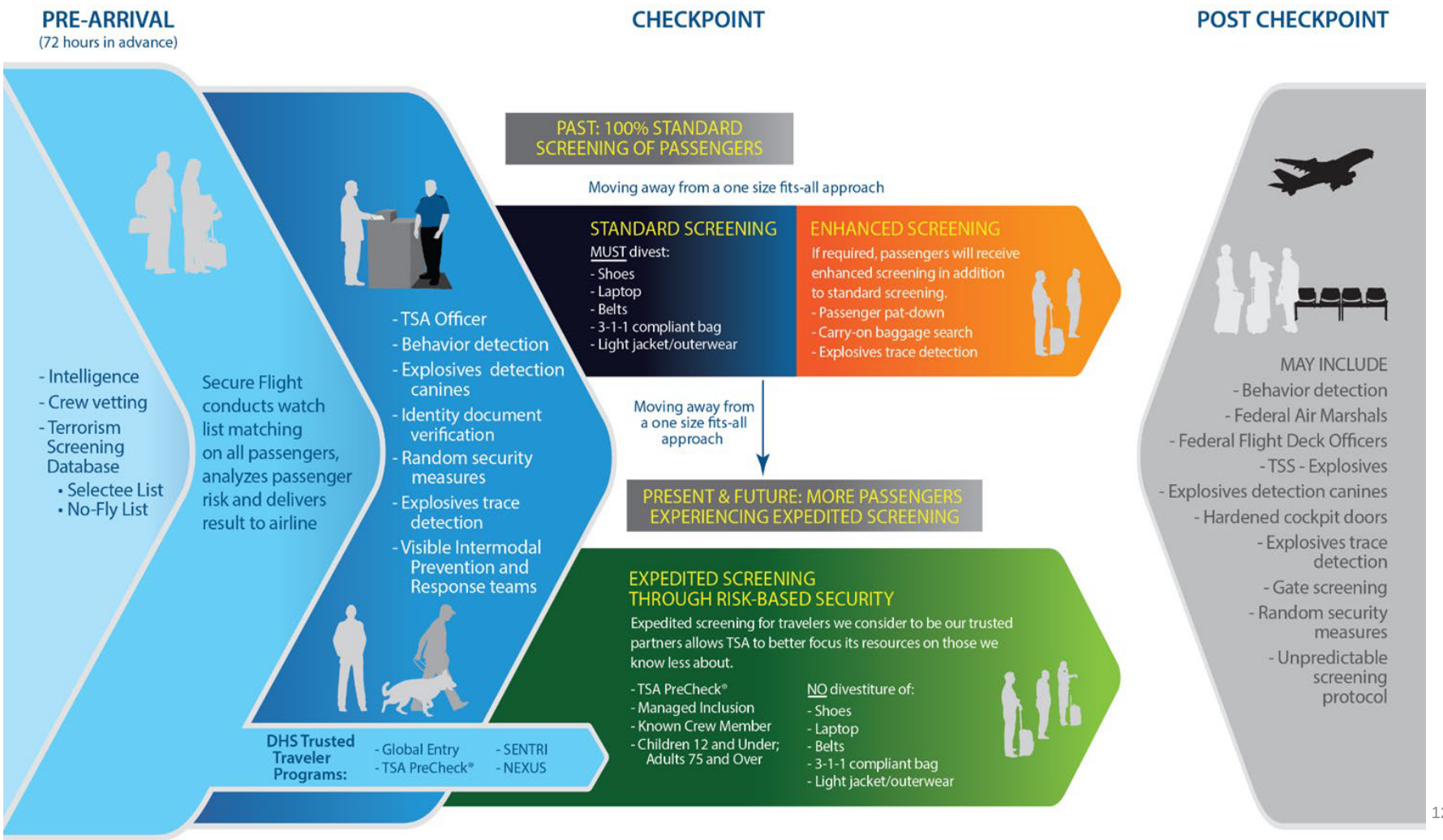
TSA STRATEGY

- Improve Security & Safeguard the Transportation System
- Accelerate Action
- Commit to Our People

Current TSA Priorities

- **Securing Airports and Commercial Aviation from Terrorism Threats**
- **Insider Threat: Aviation Worker Screening**
- **REAL ID**
- **Law Enforcement Officer and Canine Reimbursement**
- **Securing Air Cargo**
- **Cybersecurity**

Domestic Aviation Security System



Before the Airport: Pre-Screening

Risk-Based Security (RBS) Premises

- Majority of passengers are low risk, some suspected of being high risk
- Passengers who voluntarily provide more information can be better evaluated for risk
- Expediting trusted travelers improves security by allowing TSA to focus on unknown and higher risk/watchlisted travelers

Sorting Passengers Based on Known Information

- Known and Trusted Travelers – expedited screening (may leave on shoes, light outerwear, and belt, and keep laptop and 3-1-1 liquids in carry-on bag; may be screened with WTMD instead of AIT)
- Unknown Travelers – standard screening (generally screened with AIT when available)
- Higher Risk Travelers – enhanced screening (AIT screening mandatory; other additional procedures)

Secure Flight

Secure Flight Passenger Data (SFPD) – 49 CFR part 1560

- Collected by air carriers; transmitted to TSA up to 72 hours before flight
- Consists of (at a minimum) name, DOB, gender, itinerary

TSA Prescreening

- Matching against Federal government watch lists, including Terrorist Screening Center (TSC) No-Fly and Selectee Lists (49 U.S.C. 44903(j)(2))
- Matching against Trusted Traveler lists
- Passenger-specific risk assessments (PIA Update, September 4, 2013)

Boarding Pass Printing Result

- TSA sends Secure Fight pre-screening results back to air carrier
- Carriers print results on boarding passes
  - No-Fly matches denied boarding
  - Selectee matches designated for enhanced screening
  - TSA Pre✓® passengers designated for expedited screening

TSA PreCheck®

TSA PreCheck®

- Voluntary provision of biographic and biometric information and completion of criminal history background and watchlist checks
  - Members are eligible to receive expedited screening at checkpoints & TSA is able to focus resources on passengers more likely to pose a threat
- Over 30% of all travelers receive TSA PreCheck® expedited screening
  - Approximately 99% of TSA PreCheck passengers wait less than 10 minutes for screening.

Current Airport and Airline Participation

- TSA PreCheck® dedicated lanes in place at 200+ airports
- 90+ participating domestic and international air carriers
- 700+ enrollment centers

Picture Source: https://www.tsa.gov/news/press/releases/2019/09/09/tsa-prer-enrollment-offered-sioux-falls-regional-airport-one-week

Checkpoint Screening Technology

IDENTIFICATION

Credential Authentication Technology (CAT)

Boarding Pass Scanner (BPS)

ACCESSIBLE PROPERTY

Computer Tomography (CT) X-Ray

Advanced Technology (AT) X-Ray

Automated Screening Lanes

ALARM RESOLUTION

Explosives Trace Detection (ETD)

Bottled Liquids Scanner (BLS)

Chemical Analysis Device (CAD)

ON PERSON SCREENING

Walk Through Metal Detector (WTMD)

Advanced Imaging Technology (AIT) Program

Facial Recognition Technology

In support of President Biden's Executive Order on Transforming the Customer Experience, and TSA's focus on self-screening and enhanced, touchless initiatives, the following Facial Recognition Technologies (FRT) provide unique use cases for various passenger purposes:

CAT-2 with biometric camera

1:1
Credential Authentication Technology (CAT-2) with Biometric Camera

- 1:1 - Compares the image from an acceptable form of ID with the live photo of the traveler in front of the officer
- Technology: CAT-2; also mobile Driver's Licenses (mDL)
- Status: ~2,000 CAT-2 units at >80 airports in 2024
- **Key Benefit: Streamlines and further secures identity verification with limited physical interaction**

TSA PreCheck®: Touchless Identity Solution (TIS) tablet and kiosk

1:n
Touchless *PreCheck*®

- Status: ~20 units at JFK, LGA, LAX, ATL, DTW
- Only reserved for DHS Trusted Travelers who choose to opt in
- Compares a passport image – used only for the day of travel – with the live photo of the traveler in front of the officer
- **Key Benefit: Provides a fully touchless and secure identity verification experience**

Facial Recognition Technology: Privacy Protections

Key points :

- **Facial Recognition Technologies are <u>accurate</u>.**
  - TSA leverages matching algorithms developed by top-performing vendors as noted in the National Institute of Standards and Technology's (NIST) ongoing evaluation of face recognition vendor technology.
- **Facial Recognition Technology is <u>voluntary</u> for passengers.**
  - Biometric operational assessments are conducted voluntarily. For 1:1 facial matching, passengers have the right to opt-out.
  - In order to participate in 1:n matching, DHS Trusted Travelers must voluntarily provide consent by opting in to the use of facial recognition technology for identity verification purposes.
- **TSA <u>does not share or store biometric data</u> indefinitely and without reason.**
  - For 1:1 facial matching, TSA's systems do not save nor transmit any biometric data externally, except during specified data collection periods for testing and analysis by the DHS Science and Technology (S&T).
  - For 1:n matching, TSA transmits the biometric data to CBP's Traveler Verification Service (TVS) and stores the data in technical infrastructure for no more than 24 hours.
- **Accuracy in Facial Recognition Technology has increased significantly in recent years, minimizing discrepancies among diverse demographic groups.**
  - TSA works with DHS S&T to conduct demographic performance testing on a larger scale to assess the equitability of TSA's biometrics solutions.
- **TSA does not use Facial Recognition Technology to <u>profile passengers for law enforcement purposes.</u>**
  - TSA only uses biometric technology at the airport to automate the identity verification portion of the TDC process for all passengers, not for any law enforcement purposes. TSA cameras do not scan crowds and are not used for surveillance.

LEO Support for Checkpoint Screening

Deployment of Law Enforcement Officers (LEOs)

- LEOs shall be “at each airport security screening location to ensure passenger safety and national security” (49 U.S.C. 44901(h))

Airport operator responsibility

- Required to provide LEO presence (49 U.S.C. 44903(c))
  - LEOs can be state, local, or private
  - Uniformed LEOs must be provided “in the number and manner adequate to support” each checkpoint (49 CFR. 1542.215(a)(2))

Administrator’s authority to ensure LEO presence

- May designate any Federal employee as a LEO (49 U.S.C. 114(p))
- May deputize state or local LEOs to carry out any Federal airport security duty, 49 U.S.C. 44922 (currently using to deputize canine teams)

Checked Baggage Screening

Explosives Detection System (EDS)

- Automated computer tomography image capturing

TYPE 1 EDS

- Screens 400-900 bags per hour
- Officer resolves anomalies from a centralized room

1.4M Bags Daily

TYPE 2 EDS

- Screens up to 400 bags per hour
- Deployed at airports with space constraints or lower screening throughput

REAL ID

REAL ID Requirements and Preparation for Enforcement

- **Requirements:** *REAL ID Act of 2005* and DHS implementing regulation (6 CFR Part 37) set minimum requirements for State-issued driver's licenses and identification cards (DL/ID) accepted by Federal agencies for official purposes, including:
  - Accessing Federal facilities, *boarding federally regulated commercial aircraft*, entering nuclear power plants, and any other purposes that the Secretary shall determine

- **REAL ID Program Transferred to TSA**
  - Consolidated Appropriations Act of 2023: At DHS's request, Congress authorized transfer of REAL ID Program from DHS Headquarters to TSA
  - May 22, 2023: Secretary Mayorkas approved delegation officially vesting in TSA authority for implementing the REAL ID Act

- **Preparation for Enforcement**
  - **Deadline:** DHS and TSA are preparing to begin card-based enforcement **May 7, 2025**
  - TSA is currently providing a notice to travelers who present a noncompliant state ID informing them of the REAL ID start date, boarding requirements, and where they can get a REAL ID (beginning May 8)

REAL ID, Cont.

Phased Enforcement Rulemaking

- On September 12, 2024, TSA published a Notice of Proposed Rulemaking, which seeks public comment for 30 days, that would explicitly permit federal agencies, including TSA, to implement REAL ID card-based enforcement through a phased approach.
- This proposed rule seeks to ensure federal agencies, including TSA, are well positioned to begin enforcing REAL ID requirements on May 7, 2025, in a manner that meets the objectives of the REAL ID Act and regulations, while affording agencies flexibility to begin enforcement in a way that takes into account security, operational risk and public impact.
- TSA is planning for a number of scenarios, including considering a phased enforcement approach that would allow individuals to continue presenting a non-complaint DL/ID for a limited period of time. However, travelers without REAL ID-compliant ID or another acceptable form of ID should be prepared to experience some delay at TSA security checkpoints and potential impact to their travel.

Insider Threat: Aviation Worker Screening National Amendment

- **Aviation Worker Screening National Amendment**
  - In response to ASAC recommendations, TSA issued a National Amendment (TSA-NA-23-02), Apr. 27, 2023
    - Uses a risk-based approach, and takes action to mitigate persistent security vulnerabilities, address recent criminal exploits, and combat “insider threats”
  - Aviation security depends on direct involvement and close cooperation between airports and TSA

- **Industry Coordination**
  - Before issuing NA, TSA engaged with stakeholders, including airport operators and industry trade groups, to address comments after providing notice through established security program amendment process
  - TSA made changes to final amendment responsive to industry feedback

- **National Amendment Requirements**

Screening	Training
Notice	Signage
Training	Time Calculations
Explosive Detection	

Insider Threat: Aviation Worker Screening National Amendment, cont.

- **Informed Compliance**
  - Sept. 6, 2023, Notice of Informed Compliance, issued in response to stakeholder concerns raised in petitions; applies to airport operators subject to TSA-NA-23-02
  - Includes twelve-month outreach period allowing time to:
    - Develop screening plans;
    - Address hiring and budget challenges;
    - Share lessons learned and best practices; and
    - Explore potential solutions tailored to each location
  - Informed Compliance Period is now concluded
- **DHS SAFETY Act**
  - Provides liability cap when DHS determines an act of terrorism has occurred
  - Working closely with DHS SAFETY ACT Program to issue “block designation” for airports
    - SAFETY ACT Program similarly designated Certified Cargo Screening Facilities
  - Airport would certify through normal approval process, but “block designation” would speed approval by pre-determining that TSA NA procedures are covered
    - SAFETY ACT Team will consider Airport Security Program, AWS efforts and routines, and TSA Compliance record

Law Enforcement Officer (LEO) and Canine Reimbursement

- On 23 March 2024, the FY2024 budget was signed into law
- Budget largely supported TSA's requests, but did eliminate LEO Reimbursement and Canine Reimbursement programs due to budget limitations
- Each of these reimbursement agreements (Other Transaction Agreements [OTA]) was subject to the availability of appropriated funding; however, the OTAs contain language that TSA must provide a 30-day notification prior to terminating the agreement
    - All LEO and Canine agreements were terminated on 30 April 2024
- Airports participating in these programs were eligible to continue to perform services and be reimbursed through 30 April 2024, after which no expenses incurred are reimbursed
- For the Canine Program: The OTA was rewritten to provide a no cost option to the airport; under this agreement, airports continue to receive support from TSA for their Canine Teams, but the $50,500 stipend is no longer authorized
- For law enforcement services: Airports are still required to comply with the requirements of applicable regulations, Security Directives and Airport Security Programs

Recent Air Cargo Security Directives & Emergency Amendments

- **Issued in response to a heightened global threat environment**
- **Issued in close coordination with industry, interagency and international partners**
- **Worldwide implementation of heightened security requirements:**
  - Carriers must provide additional scrutiny of certain types of shipments bound for the United States
  - Carriers must collect and report additional data regarding shipments

Cybersecurity – Airport Requirements

National Amendment TSA-NA-21-05 (Jan 10, 2022)

- Designation of Cybersecurity Coordinators
- Reporting of Cybersecurity Incidents to CISA

National Amendment TSA-NA-22-01 (Jul 31, 2022)

- Have and Test a Cybersecurity Incident Response Plan (CIRP)

Jt Emergency Amendment 23-01 (Mar 7, 2023)

- Identify and List Critical Systems
- Develop and Implement Cybersecurity Implementation Plan (CIP)
- Plan for Regular Assessments of the CIP via a Cybersecurity Assessment Plan (CAP)

Cybersecurity – Emergency Status

Jt Emergency Amendment 23-01 issued on March 7, 2023 due to the continuing and evolving cybersecurity threat to aviation

- Threat is both nation states and criminal enterprises
  - Nation states prepare destructive attacks and espionage involving critical infrastructure
  - Criminal enterprises pose a lesser, but still significant threat of ransom and malware

- Ongoing emergency requires immediate and continuing action
  - Protect national and transportation security, economy, and public health and safety
  - On May 8, 2023, the Transportation Security Oversight Board informed TSA of its determination that a cybersecurity emergency existed warranting TSA's action on cybersecurity mitigation measures under its emergency regulatory authority

- Cybersecurity measures must be immediately developed and implemented
  - Aviation sector requires a level of cybersecurity commensurate with the threat

Cybersecurity – Submission Process

Airport Submission & Approval Process for CIPs and CAPs

- TSA worked with operators to develop multiple ways to satisfy submission requirements for CIPs and their incorporated documents and CAPs:
  - Provide to TSA in password-protected document
  - Provide to TSA through a secure portal
  - Retain locally for in-person inspection by TSA

Source: Joint NAM 23-01B (Feb 28, 2024)
Applies to: Category X, I, and select airport operators

Effects of Alternate Submission Options

- Cybersecurity coordinator must attest to CIP or CAP completion
- CIPs and CAPs not submitted via email are conditionally approved, pending final TSA review
- Alternative submission options do not negate or waive any TSA inspection authority

Seattle Cybersecurity Incident: August 2024

Ransomware Attack

- 11th busiest airport in U.S. by passenger volume

Systems Impacted:

- Baggage Handling
- Baggage Source Messaging
- Check-in Kiosks
- Airport display boards
- Common Use Ticketing
- Public Wi-fi
- Port of Seattle website
- flySEA app

The security of the traveling public was not impacted; TSA screened all passengers and baggage

Consequences:

- Seattle news described the scene as “chaotic” with flight delays and long lines
- 474 departing flights (1/3 of scheduled departures) were delayed in the first two days (8/24 and 8/25)
- 7,000 pieces of luggage moved manually
- Required issuance of paper boarding passes and baggage tickets
- Possible compromise of Port of Seattle employee Personally Identifiable Information

Cybersecurity – Consortia

Consortia Operated Systems

- TSA has broadened its cybersecurity requirements outside of airport and aircraft operators
- TSA issued an Order to consortia operators at 45 fueling operators at Joint EA-covered airports

Source: Order (Feb 28, 2024), issued pursuant to Title 49, Sections 114, 40113(a), and 46105(a)-(b)
Applies to: Receiving consortia operators

Other Consortia

- On Mar 1, 2024, TSA held a separate Technical Working Group with baggage handlers
- At this time, TSA will address other consortia-related challenges on a case-by-case basis

Alternate CIP Reporting for consortia subject to the Order

- If a consortia overlaps with airport or aircraft operator cybersecurity requirements, airports fill in the name and contact information for consortia subject to TSA's Order

Source: Joint NAM 23-01B (Feb 28, 2024)

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

CIRCIA Requirements for Airports

- Two criteria trigger reporting obligations for airports to CISA under proposed CIRCIA rule
  - Any airport that exceeds the Small Business Administration threshold, and
  - Any entity already required to report to TSA

Impact on TSA Requirements

- Proposed CISA rule (April 2024) does not limit TSA's scope or timeframe of reporting
- Includes exception that avoids redundant reporting if required to do another report with substantially similar content and timeframe
  - Requiring agency must enter into an information-sharing agreement with CISA
- TSA's requirements will likely be "substantially similar," but TSA will need to enter into an agreement with CISA before exception applies

Questions?

Contact information:
Francine.Kerner@tsa.dhs.gov
571-227-2693

APPENDIX

Litigation – Screening Challenges

All TSA screening falls under the ambit of the Fourth Amendment.

The U.S. Supreme Court has applied the Fourth Amendment to a wide range of searches that go beyond criminal law enforcement to meet administrative needs.

Airport searches do not need to be based on reasonable suspicion or probable cause.	***Chandler v. Miller***, 520 U.S. 305 (1997); ***NTEU v. Von Raab***, 489 U.S. 656, 675 n.3 (1989)
Requirement for travelers to present identification does not violate First or Fourth Amendment.	***Gilmore v. Gonzalez***, 425 F. 3d 1125 (9th Cir. 2006)

Screening Challenges Cont'd

The choice to attempt entry into secure area triggers screening.	***U.S. v. Aukai***, 497 F.3d 955 (9th Cir. 2007) (en banc)
Passengers must complete screening once they begin.	***U.S. v. Hartwell***, 436 F.3d 174 (3rd Cir. 2006) ***Ramsingh v. TSA*** (D.C. Cir. July 15, 2022)
Random Screening is Permissible.	***U.S. v. Marquez***, 410 F.3d 612 (9th Cir. 2005)
AIT scans "are reasonable administrative searches because the governmental interest in preventing terrorism outweighs the degree of intrusion" on privacy.	***Corbett v. TSA***, 767 F.3d 1171 (11th Cir. 2014)

Litigation – Watchlist Challenges

The weight of authority holds that selection for enhanced screening at an airport security checkpoint, whether as a result of placement on the Selectee List or for other reasons, does not deprive an individual of any constitutionally protected liberty or property interests.	***Elhady v. Kable***, 993 F.3d 208 (4th Cir. 2021); ***Abdi v. Wray***, 942 F.3d 1019 (10th Cir. 2019); ***Beydoun v. Sessions***, 871 F.3d 459 (6th Cir. 2017); ***Ghedi v. Mayorkas***, 16 F.4th 456, 466–67 (5th Cir. 2021).
The Government has unambiguous statutory authority to create, maintain, and use the terrorist watchlist.	***Kovac v. Wray***, 109 F.4th 331, 333 (5th Cir. 2024).
TSA has authority to administer its Silent Partner and Quiet Skies programs and its administration of the redress process is reasonable. (Quiet Skies covers travelers departing from domestic airports and Silent Partner pertains to persons flying into the U.S. from abroad. Individuals identified by these programs face enhanced security screening but are not considered "known or suspected terrorists.")	***Abdellatif, et al., v. DHS****, et al.,* 2024 WL 3546140 (D.C. Cir. July 26, 2024).
In FOIA, TSA may withhold information supporting inclusion on a watchlist and issue a Glomar response.	***Magassa v. TSA***, 2023 WL 8826564 (D.C. Cir. Dec. 21, 2023)

Litigation – No Fly List Challenges

The criteria for placement on the No Fly List are not unconstitutionally vague and comport with due process. Due process does not require adversarial hearings for individuals on the No Fly List.	***Kashem v. Barr***, 941 F. 3d 358 (9th Cir. 2019)
The revised DHS TRIP process satisfies Due Process requirements and sustaining TSA's decision to maintain an individual on the No Fly List.	***Busic v. TSA***, 62 F.4th 547 (D.C. Cir. 2023)
The Supreme Court affirmed a decision of the 9th Circuit holding that the Government failed to demonstrate that an individual's claims challenging his placement on the No Fly List are moot after he was removed from the No Fly List and provided a sworn TSC declaration that he would not be relisted based upon currently available information. The Supreme Court did not adopt some of the 9th Circuit's most troubling rationales, which would have effectively resulted in the Government being unable to demonstrate that any No Fly case was moot. Importantly, the Supreme Court made clear that the Government is not required to repudiate an individual's placement on the No Fly List in the first place to establish mootness.	***FBI v. Fikre***, 601 U.S. 234 (2024)

Litigation – Regulatory Challenges

In 2023, TSA took regulatory actionto secure the Watch List, require Aviation Worker Screening, and improve aviation operators' cybersecurity posture	
TSA now conducts all passenger and aviation employee vetting, including for cargo operators, 12-5 operators, and private charter operators, against the Watch List. After the "Take Back the Watch List" security program amendments were issued, TSA worked closely with operators to come into compliance.	***NetJets Aviation, Inc., Executive Jet Management, Inc., v. TSA*** (No. 23-3450, Sixth Circuit) (stipulated dismissal entered June 28, 2024)
Airport operators are required to conduct aviation worker screening in accordance with the National Amendment, with ongoing compliance efforts in effect on September 25, 2024.	***City of Billings, et al, v. TSA*** (No. 23-1290, D.C. Cir.) (motion to stay the National Amendment denied on May 28, 2024; oral argument scheduled for October 17, 2024)
Aviation operators are required to develop a Critical Infrastructure List and Plan to update and secure cyber infrastructure. One airport seeks review in the D.C. Circuit.	***Spokane Airport Board v. TSA*** (No. 23-1155, D.C. Cir.) (petition for review to be briefed this fall)

Cybersecurity – Airport Requirements

Designation of Cybersecurity Coordinators

- Designate cybersecurity coordinators as 24/7 POC with TSA

Reporting of Cybersecurity Incidents to CISA w/ TSA notice

- “Cybersecurity incidents” are events that jeopardize or are reasonably likely to jeopardize IT and OT systems
- Includes events under investigation/evaluations as possible cybersecurity incident before final determination of the event’s root cause

Source: TSA-NA-21-05 (Jan 10, 2022)

Applies to: 49 CFR 1542.103 Airport Operators

Cybersecurity – Airport Requirements, cont.

Have and Test a Cybersecurity Incident Response Plan (CIRP)

- Pre-plan organization's response to a cybersecurity incident

Source: TSA-NA-22-01 (Jul 31, 2022)

Applies to: Category X, I, and II airport operators regulated under 49 CFR § 1542.103(a); and Exclusive Area Agreement Holders regulated under 49 CFR § 1542.111

Identify and List IT and OT Critical Systems

- Identify IT or OT systems used by airport that, if compromised or exploited, could result in operational disruption
- Includes business support services that could result in operational disruption

Source: Joint Emergency Amendment (EA) 23-01 (Mar 7, 2023)

Applies to: Category X and I airport operators, and select aircraft operators

Cybersecurity – Airport Requirements, cont.

Develop and Implement Cybersecurity Implementation Plan (CIP)

- Establishes Performance-Based Measures for Critical Systems similar to pipeline and rail
- Describes fundamental cybersecurity outcomes that operators must achieve to protect against, identify, and respond to cyber threats
- Outcomes include:
  - Network segmentation policies and control
  - Access control measures
  - Continuous monitoring and detection policies and procedures
  - Timely security patches and software updates

Source: Joint EA 23-01 (Mar 7, 2023)

Applies to: Category X, and I airport operators, and select aircraft operators

Cybersecurity – Airport Requirements, cont.

Plan for Regular Assessments of the CIP via a Cybersecurity Assessment Plan (CAP)

- Assess Critical Systems to ascertain effectiveness of cybersecurity measures
- Identify and resolve device, network, and/or system vulnerabilities

Source: Joint EA 23-01 (Mar 7, 2023)

Applies to: Category X and I airport operators, and select aircraft operators