Transportation Security Administration

AAAE Basics of Airport Law Workshop
TSA Legal Update
Washington, DC

Francine J. Kerner

TSA Chief Counsel

October 30, 2018

Federal Airport Regions and Hub Locations

Transportation Security Administration

Creation of TSA

- Pre 9/11
  - Private sector screeners
  - FAA oversaw safety and security for civil aviation and regulated airports and air carriers
- Post 9/11
  - Federal screeners
  - TSA responsible to screen passengers and checked baggage
  - John Magaw stood up the Agency with a highly diverse group of professionals
  - Initially part of DOT; moved to DHS under Homeland Security Act of 2002

Leadership at DHS and TSA

- Department of Homeland Security (DHS)
  - Secretary Nominee – Kirstjen Nielsen
  - Deputy Secretary – Claire M. Grady
  - General Counsel Nominee – John Mitnick

- Transportation Security Administration (TSA)
  - Administrator – David P. Pekoske
  - Deputy Administrator – Patricia Cogswell
  - Chief of Staff – Ha Nguyen McNeill
  - Operations Support – Stacey Fitzmaurice
  - Security Operations – Darby LaJoye
  - Enterprise Support – Kimberly Walton
  - Law Enforcement/Federal Air Marshal Service – David Kohl

The Threat Continues Today

- Firearms
- Explosive Devices and Incendiaries
- Non-Metallics
- Powders
- Other Prohibited Items
- Social Engineering (e.g., passenger returns to the checkpoint on consecutive days with different stories about why they cannot undergo screening procedures)

Threat Items

Belt knife discovered at DTW in October

For more photos and stories

- blog.tsa.gov
- instagram.com/tsa

Transportation Security Administration

Current Threat Environment

- Terrorists continue to target airports and commercial aviation
- ISIS claimed responsibility for the 2015 bombing of Metrojet Flight 9268, which killed all 224 people on board; the March 2016 airport attack in Brussels, and the June 2016 airport attack in Istanbul
- With respect to aircraft, ISIS goal is to smuggle improvised explosive devices (IEDs) in various consumer items
- July 2017, Australian authorities disrupted a plot involving an attempted attack on a flight between Sydney and the UAE
  - Australian Police reported plot included an IED assembled with parts mailed via air cargo by ISIS operatives in Syria through Turkey
  - IED was hidden in a household meat grinder

Public Area Security

- New Era of Terrorism – DHS Secretary Nielsen described the threat to the world as “more numerous, more widely distributed, highly networked, increasingly adaptive, and incredibly difficult to root out.”
- Focus on Threat Environment – holistic analysis instead of just drawing the next perimeter line
- Promote Unity of Effort – coordination between all stakeholders
- Public Education– “If You See Something, Say Something”™

Addressing the Threats: TSA's Authority

- Aviation and Transportation Security Act (ATSA), P.L. 107-71 (Nov. 19, 2001)
  - TSA's Mission – Oversee security in any mode of transportation that was regulated by DOT
  - Administrator's Responsibilities – Listed in 49 U.S.C. § 114
  - TSA's Liaison Role – "Serve as the primary liaison for transportation security to the intelligence and law enforcement communities" (49 U.S.C. § 114(f)(5))

TSA Authority (cont'd)

- Screening – TSA "shall provide for the screening of all passengers and property" (49 U.S.C. § 44901)
  - Screening "shall be carried out by a Federal Government employee"
  - Exception for Screening Partnership Program (49 U.S.C. § 44919-20)
- Background Checks – Required for personnel with access to secure areas of the airport (49 U.S.C. § 114(f)(12))
- Secured Area and Perimeter Access – TSA regulates secured area access control and airport perimeter access security (49 U.S.C. § 44903(g)-(h))

TSA Authority (cont'd)

- Federal Air Marshal Service (FAMS) – Air carriers required to provide seating on any flight (49 U.S.C. § 44917)
- National Emergencies – Administrator responsible for coordinating all domestic transportation, including "transportation-related responsibilities of other departments and agencies" (49 U.S.C. § 114(g))
- Visible Intermodal Prevention and Response (VIPR) Teams – Administrator may develop "to augment the security of any mode of transportation at any location" (6 U.S.C. § 1112)

Aviation Security Screening

- Magnitude larger than you may realize
  - 43,000 Transportation Security Officers (TSOs) at 440 airports
  - 2 million passengers daily; 750 million every year
  - 1.3 million checked items; 4.9 million carry-on items
  - 23,000 domestic flights per day; 2,800 outbound international flights per day

TSA Airport Personnel

- Federal Security Director (FSD) – Oversees airport screening and carries out other duties prescribed by the Administrator (49 U.S.C. § 44933)
- Assistant FSD for Law Enforcement (AFSD-LE) – Works with Federal Law Enforcement Officers (LEOs) and helps coordinate law enforcement activities at the airport
- TSA Field Counsel – Provides legal support to FSDs on issues involving criminal and civil enforcement, liability, legal training, airport security, and personnel issues

TSA Airport Personnel (cont'd)

- Transportation Security Officers (TSOs) – Conduct administrative searches of individuals and baggage entering the sterile area of the airport and checked baggage

- Transportation Security Managers (TSMs) – Supervise TSO workforce and help resolve issues that arise during screening

- Transportation Security Inspectors (TSIs) – Investigate security incidents and compliance with regulations and, where appropriate, recommend civil enforcement actions

Key Elements of Screening to Keep Threats Out of the System

- Passenger Pre-Screening
- Physical Screening at Airport Checkpoints
- Checked Baggage and Cargo Screening

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)
  - **Watchlisted Travelers** – enhanced screening (AIT screening mandatory; other additional procedures)

TSA Pre✓®

- TSA Pre✓® – Voluntary program to provide biometric information and undergo a criminal history background check and watchlist check

- Benefits – Members are eligible to receive expedited physical screening at checkpoints & TSA is able to focus resources on passengers more likely to pose a threat

- Current Airport and Airline Participation
  - TSA Pre✓® in place at approximately 200 airports
  - 56 participating domestic and international air carriers
  - Over 350 application centers

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

- 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))
  - 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 flagged for enhanced screening; TSA Pre✓® passengers flagged for expedited screening

Quiet Skies

- Intelligence-driven, risk-based program that mitigates the threat from unknown, or partially-known, threats to security
- TSA analyzes current intelligence reporting to identify patterns of travel or other indications of higher risk, develops rules based upon this intelligence reporting, and compares passenger information to these rules to identify passengers for additional scrutiny
  - TSA's mitigation measures include enhanced screening for a defined period of time or set of circumstances, and (since March 2018) coverage of the flight by the Federal Air Marshal Service (FAMS)
  - Using Quiet Skies to inform FAM deployments leverages intelligence to more effectively use TSA's specialized assets to mitigate risks
  - FAMs have unique training to identify and mitigate threats onboard aircraft; their observations do not lead to persons being included within Quiet Skies
- Quiet Skies subject to routine review by DHS oversight offices and includes several measures to mitigate impact upon travelers

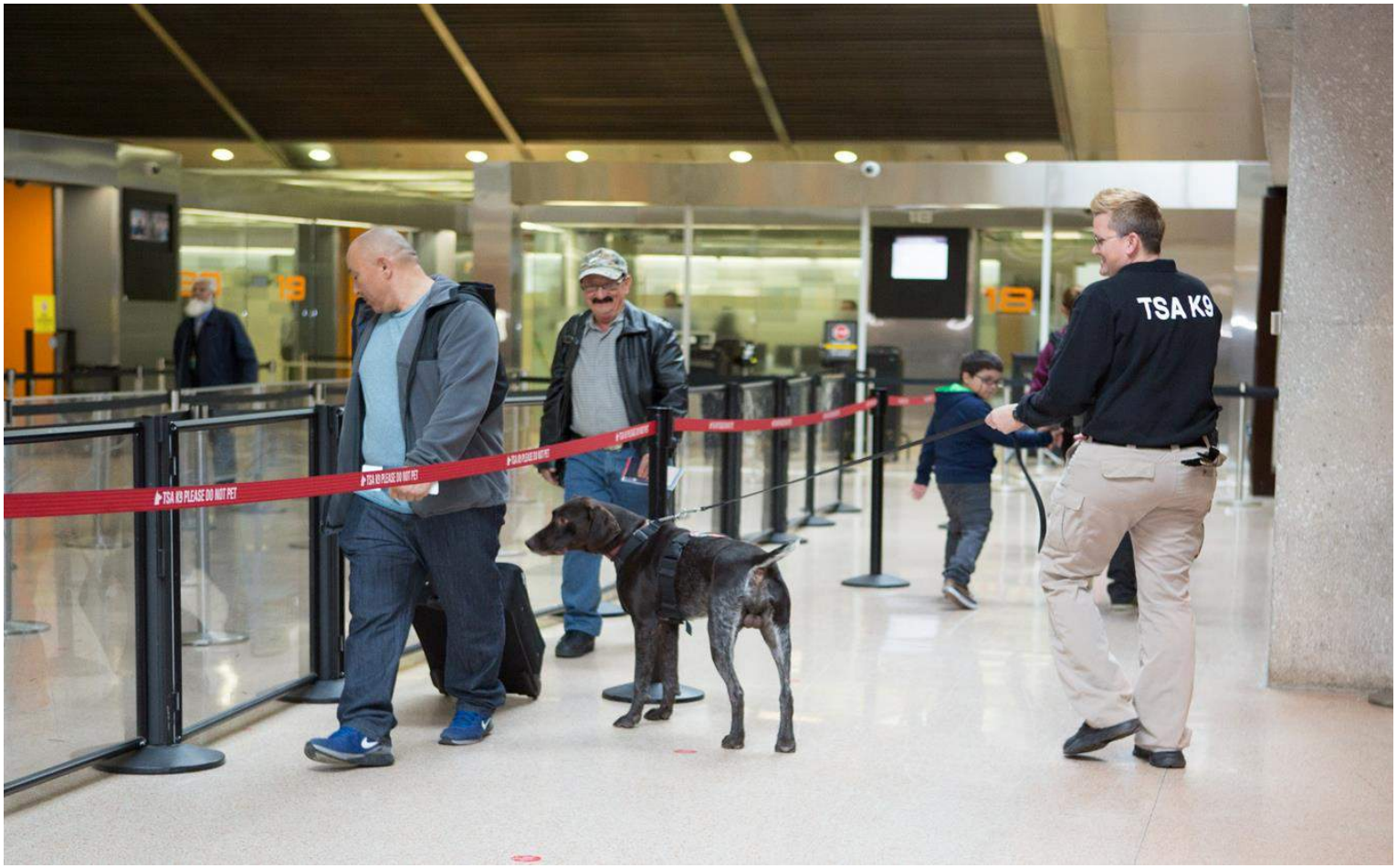
Redress Process

- DHS Traveler Redress Inquiry Program (DHS TRIP)
  - Single point of contact for travelers who believe that they were unfairly or incorrectly denied boarding or selected for enhanced screening
  - Less than 2% of cases have a connection to the watchlist
- Watchlist Status is Sensitive Security Information (SSI)
  - Generally, whether a passenger is on or off the No-Fly List or Selectee List is SSI that cannot be disclosed
  - As part of the redress process, the government may be able to disclose status on No-Fly List to U.S. Persons

After Check-In: Screening Begins in Queue

- Passenger Screening Canines (PSC)
  - TSA maximizing capacity to train and certify TSA PSC teams
  - For the first time, TSA will deputize local law enforcement officers (LEO) to carry-out Federal airport security duties under TSA supervision (49 U.S.C. § 44922)
  - Deputized local LEO canine teams will conduct screening to augment current PSC operations
  - PSC to operate under an Other Transaction Agreement (OTA) between their law enforcement agency and the National Explosives Detection Canine Team Program (NEDCTP)

Passenger Screening Canines



Transportation Security Administration

At the Checkpoint

- Screening Techniques & Technology
  - Travel Document Checker (TDC)
  - Explosives Trace Detection (ETD)
  - Walk-Through Metal Detector (WTMD)
  - Advanced Imaging Technology (AIT)
  - Pat-Downs
  - Hand-Held Metal Detector (HHMD)
  - Accessible Property X-Ray
  - Liquid Container Screening
  - Automated Screening Lane (ASL)
  - Computed Tomography (CT)
  - Credential Authentication Technology (CAT)
- Law Enforcement Support
  - Respond to refusal to complete screening & discovery of prohibited items
  - Deter and respond to incidents

Travel Document Checker (TDC)

- Identity Verification – 49 U.S.C. § 114(e) & (f)
  - TSOs required to have specialized training in document examination (9/11 Commission Act § 1611)

- TDC Implements Pre-Screening Results – checks boarding pass to determine designated level of screening

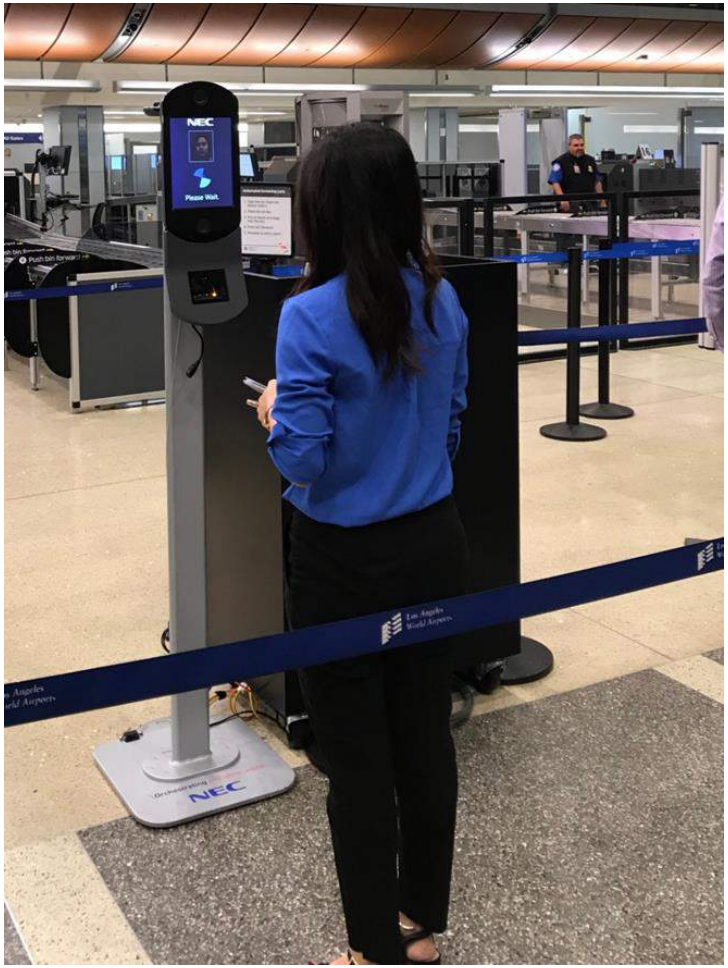
- Biometrics
  - Increasing number of alternate procedure requests from aircraft operators for passenger identification using biometrics (primarily checked baggage)
  - Current amendments permit carriers to use a biometric (facial recognition, fingerprints) to identify passengers in lieu of manual ID check required by security programs
  - TSA expects biometric trend to continue and accelerate

Facial Recognition Technology

- TSA/CBP Pilot
  - Customs and Border Protection (CBP) developing facial recognition technology to support statutorily mandated biometric entry-exit mission (8 U.S.C. § 1365b(b)(4))
  - TSA and CBP piloting CBP technology for identity verification of international travelers at TSA checkpoint
  - Future pilot phase may test data sharing between TSA (Secure Flight) and CBP (TVS) for improved passenger identification at the checkpoint
  - Passenger participation voluntary; public advised through signs, website etc.

- Verification Process
  - After photo taken at checkpoint, CBP system compares it to photo database
  - Positive match satisfies TSA's identity verification requirement, passenger proceeds to screening
  - If no match, TSA uses standard identity verification procedures before passenger proceeds to screening; CBP officers may follow-up under CBP authorities

Facial Recognition Technology



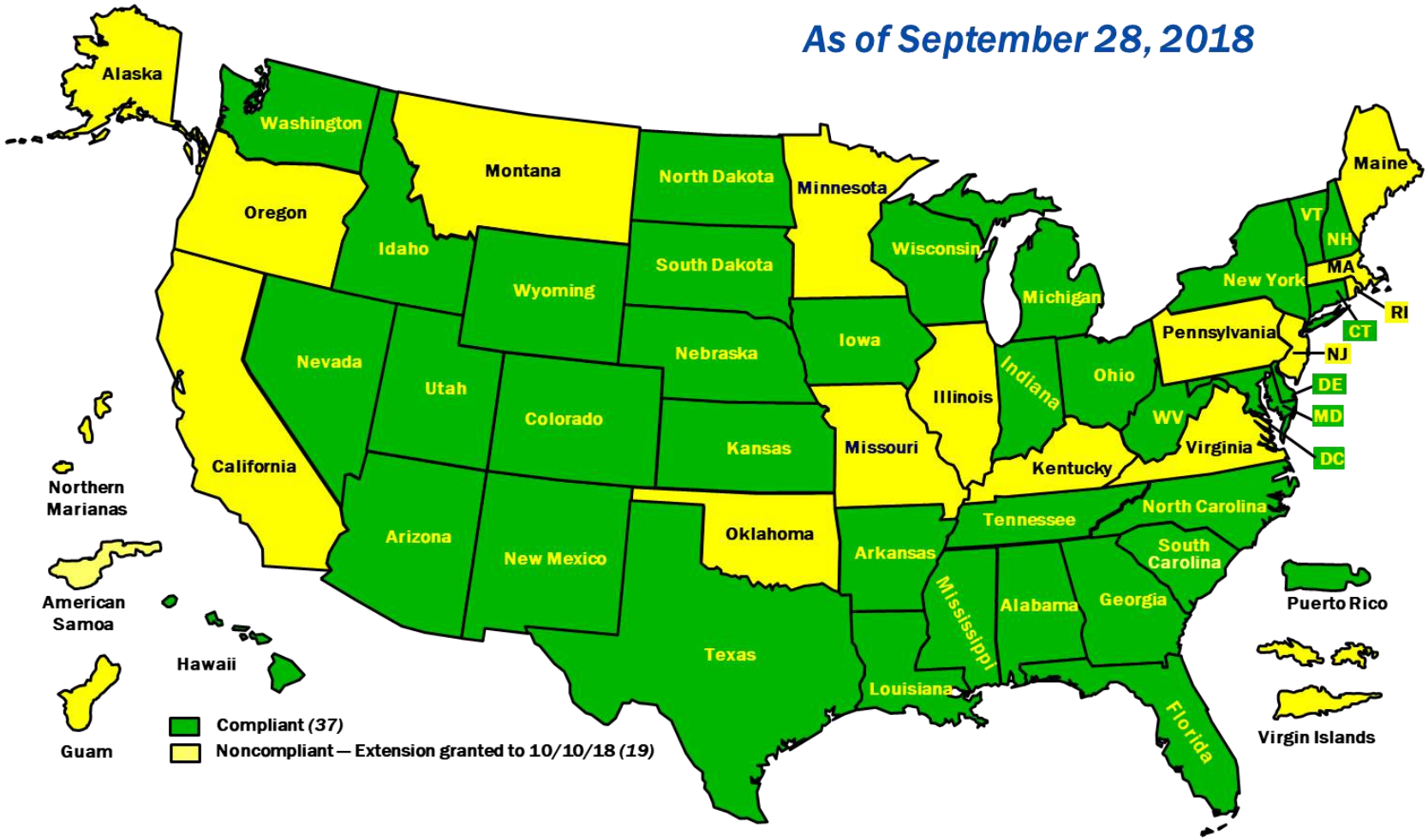
Transportation Security Administration

REAL ID Act of 2005

- Real ID Act of 2005 – Prohibits Federal agencies from accepting driver's licenses and identification cards (DL/ID) issued by noncompliant states for official purposes, including boarding federally-regulated commercial aircraft
  - As of **February 5, 2018**, TSA does not accept DL/ID issued by noncompliant states/territories that do not have an extension from DHS
  - Beginning **October 1, 2020** every commercial air traveler will need a REAL ID-compliant DL/ID (or another acceptable form of ID) for domestic air travel

- Noncompliant States/Territories With DHS Extensions
  - Alaska
  - American Samoa
  - California
  - Illinois
  - Guam
  - Kentucky
  - Maine
  - Massachusetts
  - Minnesota
  - Missouri
  - Montana
  - New Jersey
  - Northern Marianas
  - Oklahoma
  - Oregon
  - Pennsylvania
  - Rhode Island
  - Virginia
  - Virgin Islands

REAL ID Compliance Status



Improving Checkpoints – Innovation Task Force

- Innovation Task Force (ITF) Overview
  - Fosters innovation by identifying and demonstrating emerging solutions that increase security effectiveness and efficiency to inform requirements that can address security gaps in aviation security
  - Vendors submit white papers responding to Broad Agency Announcement (BAA) Problem Statements
  - TSA and airports/air carriers conduct demonstrations at "Innovation Task Force Sites" at select airports
- Previous and Current Demonstrations – Include Automated Screening Lane (ASL), Computed Tomography (CT), Biometric Authentication Technology (BAT), Enhanced Advanced Imaging Technology (eAIT), Checkpoint Planning and Staffing Allocation

Automatic Screening Lanes (ASLs)

Transportation Security Administration

Automated Screening Lanes (ASLs)

- Benefit – ASLs help mitigate checkpoint security vulnerabilities, reduce passenger congestion, and increase potential throughput of accessible property in standard screening lanes

- Passenger Throughput – Initial results demonstrate that ASLs can, at times, improve passenger throughput up to 30%

- Deployment Status – 156 ASLs at 15 airports

- Reimbursement of Services – ASLs deployed in collaboration with private sector partners leveraging TSA's reimbursement of services authority under ATSA (allows TSA to accept equipment, personnel services, and facilities from private and public partners (49 U.S.C. §114(m)))

Computed Tomography (CT)

Computed Tomography (CT)

- Baggage Screening Technology – Uses 3D-imaging and detection software to help operators automatically identify threats; eliminates need for divestiture of certain items

- Security and Efficiency Enhancements
  - Detects reduced threat mass and homemade explosives
  - Allows passengers to leave laptops, and eventually liquids, in carry-on bags
  - Increases overall checkpoint security effectiveness
  - Processes an extra 50 bags an hour

- Deployment
  - Machines in 145 airports by Fall 2019 (currently in Boston, Phoenix, New York)
  - Plans to combine with an automated conveyance system (e.g., ASLs)

- FAA Reauthorization Act of 2018 – TSA must conduct a pilot program testing the use of CT screening equipment at passenger screening checkpoints

Credential Authentication Technology (CAT)

Credential Authentication Technology (CAT)

- Technology Overview – CAT will enable near real-time cross-checking of passenger ID data, reservation data, and Secure Flight data

- Deployment Status – Currently piloting 42 units at Pre✓® lanes at 13 airports
  - Targeting full deployment at airports early 2019 (both Pre✓® and Standard lanes)
  - Conducted official DHS operational testing and evaluation (OT&E) in both Pre✓® lanes and Standard lanes in 6 airports (Austin, Boston, Indianapolis, Los Angeles, Miami, Raleigh–Durham)
  - Deployment group working with FSDs and airports to conduct site surveys collecting information on availability of active data ports and power to operate CAT at TDCs

LEO Support for Checkpoint Screening

- Deployment of 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 C.F.R. § 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)

How Courts View Security Screening

- Fourth Amendment – All TSA screening falls under the ambit of the Fourth Amendment

- Administrative Searches – 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 or "special needs"

- Legal Standard – 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)

Case Law on Basic Screening Authority

- The TDC
  - ***Gilmore v. Gonzalez***, 425 F. 3d 1125 (9th Cir. 2006) – Requirement for travelers to present identification does not violate First or Fourth Amendment
- Passengers Must Complete Screening
  - ***U.S. v. Aukai***, 497 F.3d 955 (9th Cir. 2007) (en banc) – The choice to attempt entry into secure area triggers screening
  - ***U.S. v. Hartwell***, 436 F.3d 174 (3rd Cir. 2006) – Passengers must complete screening once they begin
- Random Screening is Permissible
  - ***U.S. v. Marquez***, 410 F.3d 612 (9th Cir. 2005)

Case Law (cont'd)

- AIT is a Reasonable Search Under the Fourth Amendment
  - ***Corbett v. TSA***, 767 F.3d 1171 (11th Cir. 2014)
    - AIT scans "are reasonable administrative searches because the governmental interest in preventing terrorism outweighs the degree of intrusion" on privacy
    - AIT with Automated Target Recognition (ATR) software poses "only a slight intrusion on an individual's privacy
  - ***EPIC v. DHS***, 653 F.3d 1 (D.C. Cir. 2011)
    - Even without ATR, first generation AIT was reasonable
    - Need to search is "acute" and AIT is crucial for detecting non-metallics such as "explosives in liquid or powder form"

Case Law (cont'd)

- Selectee Watchlist Constitutional
  - ***Beydoun & Bazzi v. Sessions***, 2017 WL 4001336 (6th Cir. Sept. 12, 2017)
    - Placement on Selectee Watchlist, and additional screening measures that may occur as a result of that placement, in and of itself, does not violate substantive due process
    - Designation for additional screening likewise does not necessarily result in reputational harm, because that additional screening is an incidental or nominal burden
    - The court therefore affirmed two earlier rulings, *Bazzi v. Lynch*, 2016 WL 4525240 (E.D. Mich. Aug. 30, 2016) and *Beydoun v. Lynch*, 2016 WL 3753561 (E.D. Mich. Jul. 14, 2016)

Case Law (cont'd)

- No Fly List Constitutional
  - ***Mohamed v. Holder***, 2017 WL 3086644 (E.D. Va. July 20, 2017)
    - Even under "strict scrutiny" the No Fly List serves a compelling government interest (the "right and duty to identify . . . and stop those who present such a [terrorist] threat") that is narrowly tailored (given the procedural protections provided by DHS TRIP and judicial review)
    - The Court also explained that it expects that the DHS TRIP redress process will provide persons who believe they are on the No Fly List with an opportunity to know the reasons for their listing and to a meaningful response
    - In addition, the court expects that an administrative record will give a reviewing court the necessary information to determine whether the applicable criteria are satisfied

Pending Litigation

- No Fly List
  - ***Elhady, et al. v. Kable***, et al. (E.D. Va.) (moving towards summary judgment)
    - Procedural due process challenge to the TSC watchlist placement process and the DHS TRIP redress program available to individuals who experience travel difficulties because they believe they are on the Terrorist Screening Database (TSDB)
    - Case survived motion to dismiss-and the parties expect to file cross motions for summary judgement
  - ***El Ali, et al. v. Sessions***, et al. (D. Md.) (recently filed)
    - Challenges several aspects of Government's watchlisting regime, including standards for placement in TSDB and DHS's rules-based initiatives (Quiet Skies). Plaintiffs allege sweeping impacts of watchlisting and claim that the existing oversight and redress mechanisms – including DHS TRIP – are inadequate
    - The Complaint has been served and the Government intends to file a motion to dismiss

Pending Litigation

- *Bivens* Liability
  - ***Pellegrino v. TSA*** **(**3d Cir. 2018) (decided July 11, 2018, rehearing petition pending):
    - Following ***Vanderklok v. Kieser*** (3d Cir. 2017) (TSA screeners not personally liable for constitutional torts), court held that the Federal Tort Claims Act (FTCA) bars intentional torts arising from TSA screeners' conduct
    - Threat of liability could compromise screening, allow courts to judge TSA screening procedures based on tort considerations rather than security

Regulation of Airport Operators

- Obligation Prior/Post 9/11
  - Ensure security at airport through shared responsibility
- Airport Security Program
  - Access Control and Entry Points
  - Perimeter Security
  - Security Identification Display Area (SIDA) Badges
  - Employee Vetting and Screening
- Security Directives
- Law Enforcement Officer Support
- Protection of SSI

Airport Security Program

- Security program is required – 49 U.S.C. § 44903(c)

- Implementing Regulation – 49 C.F.R. § 1542.101
  - No person may operate an airport subject to this part unless it adopts and carries out a security program that — (1) Provides for the safety and security of persons and property on an aircraft . . . against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft

- 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"

- Regulations – Airport regulations can be found in 49 C.F.R. Part 1542

Airport Security Program (cont'd)

- Security Programs are Enforceable
  - Programs may be adopted and tailored to specific operational needs but requirements must be met
- Security Program Required Content – 49 C.F.R. § 1542.103
  - Describe sterile, SIDA, and secured areas
  - Describe measures to perform access control or to control movement within secured area
  - Develop procedures for personnel IDs, criminal history checks for persons with unescorted access
- Approval by TSA – Airport Security Program (ASP) and any amendments must be approved by TSA under 49 C.F.R. § 1542.105
- Sensitive Security Information (SSI) – Security Programs are non-public documents and are considered SSI pursuant to 49 C.F.R. Part 1520

Security Directives/Regulations

- Standard for Issuing Security Directives (SDs) – "When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures." (49 C.F.R. § 1542.303(a) (airport operators))
- Need to Know – SDs are SSI and are available only to persons with a need to know
- SDs are Mandatory – SDs supersede Security Program provisions and have the force and effect of a regulation
- Reporting to Congress – Aviation Security Act of 2016 § 3409 requires informing Congress of all SDs and how they respond to specific threats

Regulatory Enforcement

- Civil Penalties – TSA has authority under 49 U.S.C. §§ 114 and 46301 to assess civil monetary penalties of up to $13,333 per violation, per day (exception: maximum penalty is up to $33,333 per violation, per day for air carriers which are not small business concerns)

- Potential Enforcement Actions – TSA may use on-the-spot counseling, warning notice or letter of correction, civil penalty action, or security program withdrawal

- Notification to Alleged Violators – TSA notifies alleged violators of the allegation and gives an opportunity for response; violators may then appeal to an ALJ and subsequently to the TSA Decision Maker and then the Courts of Appeals

2018 UPDATE: Action Plan Policy and Progressive Enforcement

- Action Plan Program Policy Overview – TSA drafting revised Action Plan Policy to help entities address noncompliance prior to, or instead of, TSA taking formal enforcement action

- Prior Program History
  - October 1, 2017, TSA introduced new enforcement strategy (“Outcome Focused Compliance”) encouraging TSA and entities to address security vulnerabilities jointly through corrective actions
  - Policy applied to three scenarios (“initiatives”): (1) "Voluntary Disclosure Program Policy (entity discloses violation); (2) TSA Resolution Corrective Action Policy (TSA identifies violation); and (3) Vulnerability Mitigation Policy (TSA or regulated entity recognizes vulnerability before it becomes a violation)
  - Feedback: program too complicated; TSA streamlining into one Action Plan Policy

- New Program Highlights
  - Eligible parties and TSA will collaborate and jointly address: (1) noncompliance before TSA issues a Letter of Investigation (LOI); and (2) security vulnerabilities not addressed in regulations
  - Generally will not apply to egregious or intentional noncompliance or to those instances involving criminal activity or fraud

Protecting Sensitive Security Information

- Definition (49 C.F.R. § 1520.5) – SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would:
  - Constitute an unwarranted invasion of privacy
  - Reveal trade secrets or privileged or confidential information
  - Be detrimental to the security of transportation
- Covered persons – authorized to access SSI (49 C.F.R. § 1520)
  - Airport and aircraft operators
  - Indirect air carriers (IACs)
- Duty to protect – Covered persons have a duty to protect SSI
- Requests for SSI – TSA works closely with airports to protect SSI when there are 3rd party requests for information

SSI Handling

- Proper Handling of SSI (49 C.F.R. § 1520.9)
  - Take reasonable steps to safeguard SSI – store in a secure container or locked room
  - Disclose only to covered persons with a need to know – covered persons must disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing
- Requests for SSI – Refer to TSA or applicable agency in DOT or DHS
  - Consulting with the responsible agency is required under 49 U.S.C. § 1520.9(a)(3)
- Marking and Disposal of SSI – Follow 49 C.F.R. § § 1520.13 & 1520.19
- Dealing with Unmarked SSI – Mark and inform sender
- Unauthorized Disclosure of SSI – Report to TSA or applicable agency

Secured Area and Perimeter Security

- 49 U.S.C. § 44903(g)–(h) – TSA has authority to improve secured area access control and airport perimeter access security

- Background Checks – TSA requires background checks for personnel with access to secure areas of the airport. 49 U.S.C. § 114(f)(12)

- Access Control – Airport operators control access to many areas, such as from the public areas to the sterile area or secured area, and from the secured area to the sterile area. Persons are allowed access based on airport-issued ID and/or access media. Human guards and/or technology such as electronic locks can be used to secure area
    - Secure Identification Display Area (SIDA) Badges

Seattle-Tacoma International Airport Plane Theft

- Incident Overview
  - August 10, 2018, Horizon air ground service agent, without authorization, removed empty aircraft from maintenance position at Seattle-Tacoma International Airport
  - Employee flew for about an hour, pursued by two F-15 fighter jets, and crashed about 30 miles from the airport on Ketron Island
  - Employee had a valid Security Identification Display Area (SIDA) credential

- Status
  - Current investigations underway by TSA, FBI, and NTSB
  - TSA will work with government and industry partners to identify and address vulnerabilities exploited by this incident
  - Best practices/potential security requirement changes to be considered by the Aviation Security Advisory Committee (ASAC), Insider Threat Subcommittee

Advanced Threat Local Allocation Strategy (ATLAS)

- ATLAS History
  - Responds to ASAC recommendations and FAA Extension, Safety, and Security Act of 2016 (FESSA) requirements that TSA develop a model and best practice for airport worker unescorted access
  - Replaced Playbook; ATLAS more intelligence-based

- Current Operations
  - TSA requires ATLAS in certain airports based on risk; FSDs have discretion to use at remaining airports in coordination with airport operators
  - TSA develops “Randomized” and “FSD-Directed” operations
  - ATLAS produces daily schedule for Aviation Worker Screening at Direct Access Points (DAPs) and throughout security restricted areas and gates
  - Airport workers subject to random physical security inspections (persons, property)
  - Local stakeholder partnerships encouraged – “whole of community” effort

Airport Access and Vetting National Amendment

- National Amendment Overview
  - TSA assuming responsibility for terrorism-related watchlist matching through Airport Access and Vetting National Amendment (NA) (historically done by airport operators)
  - NA issued June 25, 2018 and effective July 25, 2018

- Key Provisions
  - TSA will conduct watch list matching for: (1) non-traveling individuals seeking access to airport sterile area (e.g., escorts); (2) other individuals authorized to conduct business at the airport (e.g., construction worker); and (3) airports without a personnel identification system in their Airport Security Program (ASP)
  - Available vetting options: (1) connection to Secure Flight (DHS router); (2) connection to E-Secure Flight (web portal); or (3) submission via TSA-approved service provider (contract or to aircraft operator)
  - Data transmitted to TSA must be used only for official security purposes

FAA Extension, Safety, and Security Act of 2016

- Highlighted Requirements
  - Fully implement Rap Back
  - Revise SIDA access regulations to strengthen eligibility requirements for access to secured areas
  - Authorize airport operators to have direct access to E-Verify and Systematic Alien Verification for Entitlements (SAVE)
  - Ensure that airports report unaccounted for SIDA media

Rap Back

- FESSA Mandate – TSA required to fully implement Rap Back (in place at 137 airports, 3 airlines)
  - Participation currently voluntary pending TSA proposed security program change mandating Rap Back participation

- Operational Overview
  - Improves criminal vetting by providing real-time notification of new criminal activity (arrests, convictions, some warrants) without need to submit new fingerprints
  - Airport "enrolls" individual into Rap Back when submitting an individual's fingerprints to FBI; FBI runs fingerprints against criminal database on a recurrent basis and provides Rap Back information to airports through TSA portal
  - Rap Back retrieves want/warrant information only if the individual's fingerprints are in the criminal history database

FBI's Air Domain Computer Information Comparison (ADCIC)

- ADCIC Overview
  - FBI offers ADCIC to airports to help detect insider threats (voluntary)
  - Vets against State wants/warrants (name-based) to identify workers who may have committed crime, but not yet arrested; does not check conviction/arrest database; checks missing persons file
  - Airport provides worker's biographic information to FBI; FBI provides real-time notice of want/warrant back to airport

- TSA Interpretation
  - June 2018, TSA Chief Counsel issued interpretation stating that regulations do not limit sharing records with FBI; interpretation included designation from the Administrator that airports may share criminal records with FBI

- Airport Access to FBI Wants/Warrants (Without ADCIC)
  - Airports want to submit individuals' biographic and fingerprints only to TSA rather than to both TSA and FBI; TSA awaiting response from FBI as to whether technology can link criminal database with wants/warrant database

Amending Vetting Requirements for SIDA Access

- FESSA Requirements – TSA must: (1) propose lookback period of 15 years from conviction or 5 years from release from prison; (2) revise the list of disqualifying crimes; (3) develop appeal and waiver program; and (4) consider adopting CBP and TWIC/HME disqualifying offenses

- Rulemaking Status – Notice of Proposed Rule (NPRM) estimated August 2019

- Industry Input – Aviation Security Advisory Committee (ASAC) Insider Threat Working Group recommendations to be considered in NPRM

- START Study – TSA collaborating with FBI and the National Consortium for the Study of Terrorism and Responses to Terrorism (START) (DHS Center of Excellence, led by University of Maryland and comprised of international scholars); studying patterns of criminal behavior that precede or coincide with terrorist activity

Improve Vetting of Immigrant Workers

- Airports Have Direct Access to SAVE & E-Verify
  - DHS, USCIS, and TSA have coordinated to provide airport operators with direct access to SAVE—meeting FESSA mandate
  - **SAVE** provides electronic immigration status verification information; typically available to federal, state, and local benefit-issuing agencies (e.g., DMVs)
  - **E-Verify** provides electronic work authorization information; employers have always had access by inputting information directly from a new hire's Form I-9

Airport Identification Media Audits ASP Amendment

- Amendment Overview
  - Pursuant to FESSA and DHS OIG badge audit recommendations, TSA requiring airport operators to report any time they exceed specified SIDA badge loss rate (3% CAT X, 5% others) and clarifying how airports can conduct badge audits (including badge counting) (SIDA badge audit currently required by Security Directive (SD))
  - Amendment will maintain SD requirement that all airports re-issue badges in cases of 5% badge loss rate

- Amendment Status
  - Originally distributed for comment December 4, 2017, TSA incorporated substantive stakeholder recommendations and re-issued amendment for comment September 21, 2018, final amendment estimated early November

FAA Reauthorization Act of 2018 (October 5, 2018)

- TSA Administrator – Establishes a five-year term for TSA Administrator
- TSA Pre✓® – Requires TSA to leverage private sector to make TSA Pre✓® enrollment easier for passengers; meet targets for expanding TSA Pre✓® enrollment; and ensure only trusted traveler program participants (or certain low risk passengers traveling with program participant) use TSA Pre✓® security screening lanes
- Air Cargo Security Division – Requires TSA to establish an air cargo security division to carry out air cargo policy and stakeholder engagement
- Screening Equipment Testing – Requires TSA to develop and implement a program allowing for third party operational and detection testing and verification of security screening technology as an alternative to TSA's processes; prioritize field testing and evaluation (including third-party) as an alternative to the TSA Systems Integration Facility
- Wait Times – Requires TSA to make real-time information on wait times publicly available
- Canines – Includes requirements related to canine breeding, third-party canine standards and use, and digital monitoring of canine training and testing

Questions?

Contact information:

Francine.Kerner@tsa.dhs.gov

571-227-2693