

Ground Truth Brief

SOAA
SPECIAL OPERATIONS
ASSOCIATION OF AMERICA

Threats to U.S. Aviation Infrastructure

A TSA 2026 Strategy-Anchored
Threat Landscape and Legislative Analysis

I. EXECUTIVE SUMMARY 3

II. TSA'S 2026-2030 NATIONAL STRATEGY & THREAT LANDSCAPE OVERVIEW 5

PART ONE: RISKS TO AVIATION 7

III. Improvised Explosive Devices, Mass-Casualty, Landside Attacks 7
IV. Standoff Weapons Attacks 9
V. Hijacking 11
VI. Insider Threats 13
VII. Unmanned Aircraft Systems 16
VIII. Cybersecurity 21
IX. Sabotage at Maintenance Facilities 23

PART TWO: RISKS AROUND AVIATION 24

X. Transnational Crime Exploiting Aviation Infrastructure 24
X.A Human and Child Trafficking 24
X.B Drug Smuggling 25
X.C Illicit Cash / Bulk Currency Smuggling 25
X.D Cartel Drone Use 26

XI. OSINT-REPORTED INCIDENTS, UNVERIFIED AND NON-CREDIBLE THREATS 28

XIII. LEGISLATIVE LANDSCAPE 30

H.R.2353, Safer Skies Act of 2025 30
S.3481, Counter-UAS SAFER SKIES Act (Distinct, Enacted Bill) 32
H.R.8770, SAFEGUARDS Act of 2026 32
H.R.9391, Reimbursable Screening Services Program (RSSP) Extension Act of 2026 32
H.R.9388, One-Stop Pilot Program Extension Act 33
S.1180 — Abolish TSA Act 33

XV. AUTHOR BIOGRAPHY 35

XVI. SOURCING APPENDIX 36

I. Executive Summary

The Transportation Security Administration published a 2026-2030 National Strategy for Transportation Security. This report details explicit threats to our nation's transportation sectors with additional aviation specific threats. The goal of this report is to document the threats to aviation security, provide an in-depth open-source intelligence analysis of the threat landscape and define the legislative steps currently being taken to address those gaps.

- Improvised Explosive Devices, Mass-Casualty, Landside Attacks — 7 incidents
- Standoff Weapons Attacks — 3 incidents
- Hijacking — 2 incidents
- Insider Threats — 7 incidents
- Unmanned Aircraft Systems — 12 incidents
- Cybersecurity — 5 incidents
- Sabotage at Maintenance Facilities — 1 incident
- Human and Child Trafficking — 2 incidents
- Drug Smuggling — 3 incidents
- Illicit Cash / Bulk Currency Smuggling — 3 incidents
- Cartel Drone Use — 1 incidents
- OSINT Reported Incidents, Unverified — 7 incidents

TSA's security system does more than stop threats at the checkpoint. Their presence deters activity from the channels it covers and pushes it toward channels it does not. This dynamic surfaces repeatedly throughout this report. The Drug Enforcement Agency's own aviation division has stated that traffickers increasingly favor private aviation specifically to avoid commercial screening. The limited case records in the Standoff Weapons and Maintenance Sabotage sections are evidence of deterrence rather than an absent threat.

Among the legislative responses documented in this report, H.R.2353, the Safer Skies Act of 2025 (distinct from the enacted counter-UAS SAFER SKIES Act, S.3481), is the most direct attempt to close the screening-tier gap that displacement dynamic exploits. The bill would require certain public charter operations currently screened under the lighter Twelve-Five Standard Security Program (TFSSP) to meet the full Aircraft Operator Standard Security Program (AOSSP) standard applied to scheduled commercial carriers. Within its scope, the bill would directly strengthen security against several threat categories documented in this report: it would close an unscreened entry point relevant to improvised explosive devices and weapons, eliminate a boarding pathway subject to less scrutiny than traditional terminals in the hijacking category, and extend commercial-grade screening and detection protocols to a channel that traffickers and bulk-cash couriers currently treat as lower-scrutiny. Section XIII assesses its impact against each threat category in this report individually.

The legislative landscape is constantly evolving. Not every bill covers the same challenges nor expands TSA's authority, though. This demonstrates a clear understanding of the threat but not total alignment on the solutions. Visit the Special Operations Association of America website, soaa.org, to follow our continuing work of assessing national security threats and informing policymakers on Capitol Hill.

This report is built entirely from open-source material and carries the limitations inherent to that method. The OSINT-Reported Incidents section documents threats later assessed as non-credible and should not carry the same evidentiary weight as adjudicated cases elsewhere in this report. This is a point-in-time snapshot of an active legislative and threat environment.

II. TSA's 2026-2030 National Strategy & Threat Landscape Overview

The Transportation Security Administration has a singular mission: to protect the nation's transportation systems to ensure freedom of movement for people and commerce. The TSA was founded in 2001 in direct response to the 9/11 attack. In the quarter century since, the threat landscape TSA was built to fight has evolved to a multi-dimensional threats landscape.

The TSA regularly updates its National Strategy for Transportation Security to Congress. On July 16, 2026, TSA submitted its strategy covering calendar years 2026 through 2030. The strategy sets three distinct goals for the Transportation Systems Sector:

1. advance risk-based, intelligence-driven, layered security across all transportation modes
2. modernize screening and credentialing technology to protect the homeland, borders, and key supply chain nodes
3. and strengthen cybersecurity posture and resilience of national transportation infrastructure

This document cites two specific and current events as evidence of an escalating and increasingly hybrid threat picture. The first is Iran's targeting of civilian airports and energy infrastructure in the Middle East in March-April 2026 as an example of the large-scale destructive impact sophisticated nation-states can have on transportation systems. The second event is Houthi forces in Yemen adopting military-grade unmanned aircraft systems to target aviation in the region, a tactic historically associated with nation-states rather than non-state actors. The strategy frames these events as evidence that the line between nation-state and non-state tactics is eroding, a dynamic it expects to continue shaping the threat environment through 2030.

The strategy's sector-wide risk profile names six key risk drivers of risk in America’s transportation sector:

Improvised Explosive Devices: Person-borne or vehicle-borne devices placed in baggage, cargo, or vehicles near terminals and fueling areas to damage aircraft or infrastructure.

International and Domestic Terrorists: Actors who hijack aircraft, use aircraft as weapons, deploy standoff weapons, stage mass-casualty attacks in open public areas, or move chemical, biological, radiological, and nuclear (CBRN) materials through cargo.

Insider Threats: Individuals with authorized access to secure areas, systems, or information who exploit or enable exploitation of that access to facilitate an attack.

Unmanned Aircraft Systems: Widely available drones capable of delivering explosives or CBRN agents at standoff range, conducting surveillance, or launching cyber intrusions, while remaining difficult to detect.

Cybersecurity: Malicious or accidental cyber intrusions into the information and operational technology that runs air traffic control, airport operations, and baggage handling.

Emerging Technology: New and cross-sector capabilities that can introduce novel vulnerabilities or worsen existing ones, such as autonomous vehicles, advanced air mobility, AI, quantum computing, or the Internet of Things.

The aviation-specific modal plan narrows this further to seven named categories:

1. improvised explosive device attacks
2. standoff weapons attacks
3. hijacking
4. insider threats
5. UAS interference (kinetic and non-kinetic use)
6. cyberattacks
7. sabotage at maintenance facilities

This report is organized directly around those threat categories, followed by a second section addressing transnational crime that exploits aviation infrastructure without necessarily attacking it.

Sources

- ODNI — 2025 Annual Threat Assessment (unclassified)
- HSToday — summary of ODNI 2025 Annual Threat Assessment

PART ONE: RISKS TO AVIATION

III. Improvised Explosive Devices, Mass-Casualty, Landside Attacks

TSA's strategy names IEDs, both person-borne and vehicle-borne, as a threat to aviation and surface assets. The report also identifies open and crowded public areas such as ticketing halls, baggage claim, and airport connections as vulnerable to small arms, edged weapons, explosives, and CBRN attacks. This section covers both halves of that risk driver together, since the confirmed U.S. case record for aviation-adjacent mass-casualty violence sits almost entirely in these unscreened landside spaces rather than past a checkpoint.

Incident Detail

Thwarted Hartsfield-Jackson Attack (October 2025)
A man's own family alerted Atlanta police that he was armed and headed to Hartsfield-Jackson intending to open fire in the terminal while livestreaming; an officer recognized him from the family's description and made the arrest before he reached a crowd.

Fit/Limitations: Demonstrates landside vulnerability and the role of non-law-enforcement tips in disruption; confirmed arrest, but underlying threat severity relies on self-reported family account rather than independent verification.
Source: https://www.cnn.com/2025/10/23/us/atlanta-airport-threat-safety-security

Fort Lauderdale-Hollywood Airport Shooting (January 6, 2017)
An armed attacker opened fire in the Terminal 2 baggage claim area, killing five people and wounding six more.

Fit/Limitations: Attack occurred entirely within an unscreened landside space with no checkpoint involved at any point, the clearest domestic example of landside mass-casualty risk in this section. Confirmed, adjudicated.
Source: https://www.justice.gov/usao-sdfl/pr/esteban-santiago-ruiz-sentenced-life-prison-connection-shooting-fort-lauderdale

LAX Terminal 3 Shooting (November 1, 2013)
A gunman entered LAX Terminal 3 and killed TSA Officer Gerardo Hernandez, wounding two other TSA officers and a civilian, before being apprehended.

Fit/Limitations: Shooter moved through landside terminal areas before reaching the checkpoint, direct evidence that screened checkpoints do not cover the full terminal environment. Confirmed, adjudicated (DOJ sentencing).
Source: https://justice.gov/opa/pr/california-man-sentenced-life-plus-60-years-2013-shooting-spree-los-angeles-international

JFK Airport Jet-Fuel Tank Bomb Plot (2007):
A plot to bomb jet-fuel supply tanks at JFK Airport was disrupted; a former airport employee among the conspirators used his knowledge of the site to conduct surveillance and identify targets and escape routes.
Fit/Limitations: Illustrates IED and insider-threat categories intersecting directly, discussed further in Section VI. Confirmed, adjudicated case.
Source: https://www.aljazeera.com/news/2007/6/3/us-foils-plot-to-bomb-airport

LAX El Al Ticket Counter Shooting (July 4, 2002)
A gunman opened fire at the El Al ticket counter inside LAX's Tom Bradley International Terminal, killing two people before being shot by an El Al security guard.

Fit/Limitations: Occurred before any TSA screening point existed in the passenger's path.
Source: https://www.latimes.com/archives/la-xpm-2002-jul-07-me-lax7-story.html

U.S. Airport Criminality, General Case Study
Aggregated case study reviewing landside criminal activity patterns across U.S. airports.

Fit/Limitations: Supports the broader landside-vulnerability pattern rather than a specific threat or incident.
Source: https://www.ospreyflightsolutions.com/casestudy/criminality-at-us-airports

Grayline Intelligence Tracker, HAYI/IRGC Dataset
Owned OSINT dataset documenting 36 qualifying incidents tied to the Iranian proxy and broader gray-zone threat signature, with 27 fatalities, 56 injuries, and 14 plots disrupted before execution; includes the HAYI network's hybrid campaign, which has favored low-visibility local recruits over hardened operational cells.

Fit/Limitations: Corroborates the landside/low-scrutiny pattern from a state-linked angle rather than a lone-actor angle, shows the same vulnerability being exploited by a different category of threat actor. Primary dataset; confidence-scored per Grayline's own methodology, not independently adjudicated like the DOJ cases above.
Source: https://graylineintel.com

Sources

- Al Jazeera — JFK Airport fuel-tank bomb plot (2007)
- CNN — thwarted Hartsfield-Jackson attack (Oct 2025)
- Osprey Flight Solutions — U.S. airport criminality case study
- DOJ — Fort Lauderdale shooting sentencing
- DOJ — LAX 2013 shooting sentencing
- https://www.latimes.com/archives/la-xpm-2002-jul-07-me-lax7-story.html
- Grayline Intelligence tracker (primary dataset, owned platform)

IV. Standoff Weapons Attacks

TSA, the FBI, and the broader U.S. intelligence community have treated MANPADS proliferation as a top national security priority since at least the early 2000s. The absence of a successful standoff-weapons attack on U.S. commercial aviation over more than two decades is plausibly a measure of sustained interdiction and intelligence effectiveness, not an indication that the underlying threat capability or intent has gone away.

TSA names standoff weapons, specifically Man-Portable Air Defense Systems (MANPADS), rocket-propelled grenades, and anti-tank guided missiles, as a distinct threat category, capable of targeting aircraft and airport facilities from outside the perimeter during the most vulnerable phases of flight: takeoff and landing. The confirmed U.S. case record for this category is narrow but real.

In 2003, British arms dealer Hemant Lakhani was arrested in Newark, New Jersey attempting to sell a shoulder-fired SA-18 Igla missile to an FBI informant posing as a member of a Somali militant group after a 22-month multinational sting operation. Lakhani believed the missile would be used to shoot down a U.S. commercial airliner and told the informant he understood the economic damage such an attack would cause. He was sentenced to 47 years in prison. No confirmed U.S. case involving an actual RPG or anti-tank guided missile attack against commercial aviation has been identified, and this report states that gap directly rather than implying equivalence between the three named weapon types.

A May 2025 Congressional Research Service report on TSA funding confirms continued federal attention to "aircraft vulnerabilities to shoulder-fired missiles and other external threats, such as rocket-propelled grenades," alongside parallel work on UAS-related airport vulnerabilities. The same report notes that TSA's aircraft-mounted counter-MANPADS defense systems were tested and FAA-certified by 2009, but have never been deployed on U.S. commercial airliners, primarily due to acquisition and life-cycle cost.

Incident Detail

LaGuardia Airport Shoulder-Fired Missile Alert (July 22, 2026)
Air traffic controllers issued a security bulletin to pilots inbound to LaGuardia, warning of a possible individual carrying a rocket launcher near the final approach path; crews were told to watch for suspicious activity on the ground. The threat was later assessed as non-credible.

Fit/Limitations: Most recent activity tied to this threat category, but unconfirmed; no device or individual was ever verified. Fuller narrative treatment lives in Section XI (OSINT-Reported Incidents, Unverified and Non-Credible Threats)
Source: https://aeroxplorer.com/articles/laguardia-tower-alerts-pilots-to-possible-shoulderfired-missile-threat-near-airport

CRS Report R48543, Funding Aviation Security and TSA Screening Functions (May 2025)
A Congressional Research Service report confirms continued federal attention to aircraft vulnerabilities from shoulder-fired missiles and other external threats such as RPGs, and notes that TSA's aircraft-mounted counter-MANPADS defense systems were tested and FAA-certified by 2009

but have never been deployed on U.S. commercial airliners, primarily due to acquisition and life-cycle cost.

Fit/Limitations: Not an incident; a current (2025) federal policy document confirming this remains an active, named concern independent of incident volume. Explains why the category persists in TSA's threat framework despite a thin case record.
Source: https://www.congress.gov/crs_external_products/R/HTML/R48543.html

Hemant Lakhani MANPADS Sting Operation (2003)
British arms dealer Hemant Lakhani was arrested in a Newark, New Jersey hotel room after a 22-month multinational sting operation, in the course of attempting to sell a shoulder-fired SA-18 Igla missile to an FBI informant posing as a member of a Somali militant group; Lakhani believed the missile would be used to shoot down a U.S. commercial airliner and told the informant he understood the economic damage such an attack would cause.

Fit/Limitations: The only confirmed U.S. case directly tied to standoff-weapon intent against a commercial airliner. Sting-based, not an intercepted operational plot, the missile and buyer were both undercover; useful as evidence of intent and black-market accessibility, not of an active domestic supply network.
Source: https://www.baltimoresun.com/2003/08/14/fbi-affidavit-details-months-of-talks-that-led-to-arms-sting/

Sources

- Baltimore Sun — FBI affidavit details Lakhani sting operation
- Redorbit — Hemant Lakhani sentenced to 47 years
- FBI — criminal complaint filing announcement, Hemant Lakhani
- Congress.gov / CRS — R48543, Funding Aviation Security and TSA Screening Functions (May 2025)
- GAO-04-728 — Aviation Security: airport perimeter and access control review

V. Hijacking

TSA, the FBI, and the broader U.S. intelligence and law enforcement community have treated hijacking as the foundational aviation security threat since before TSA's creation. The post-9/11 layered security model reflects two decades of sustained investment specifically against this threat. The rarity of hijacking incidents against U.S. commercial aviation since September 11, 2001 is plausibly a measure of that sustained investment and interdiction effectiveness, not evidence that the underlying threat has diminished.

TSA names hijacking and the use of aircraft as weapons as a core risk driver within its "international and domestic terrorists" category. The strongest current U.S. case is Cholo Abdi Abdullah, sentenced to life in prison in December 2025 for conspiring on behalf of al-Shabaab to hijack a commercial airliner and crash it into a building on U.S. soil. The DOJ's own language describes this plot as an attempt to replicate the September 11 attacks.

Most recently, on May 30, 2026, a passenger aboard United Flight 2005 from Chicago to Minneapolis allegedly attempted to breach the cockpit door while ranting in Russian. The aircraft squawked code 7500, the standard transponder signal for an in-progress hijacking, and diverted to Madison, Wisconsin, where the subject was detained by the Dane County Sheriff's Office with FBI Milwaukee's Madison Resident Agency responding.

Incident Detail

United Flight 2005, Attempted Cockpit Breach (May 30, 2026)

A passenger allegedly attempted to breach the cockpit door while ranting in Russian aboard a United flight from Chicago to Minneapolis; the aircraft squawked code 7500 and diverted to Madison, Wisconsin, where the subject was detained.

Fit/Limitations: Most recent domestic incident in this category and the only one where the crew and ATC treated the event as an actual hijacking attempt in real time (via the 7500 squawk), distinguishing it from the unruly-passenger incidents in Section XI. No confirmed prosecution outcome as of this draft.
Source: https://www.wisn.com/article/passenger-arrested-after-hijack-scare-forces-emergency-landing-in-madison/71451242

Cholo Abdi Abdullah, al-Shabaab Hijacking Plot (Sentenced December 2025)

Abdullah was sentenced to life in prison for conspiring, on behalf of al-Shabaab, to hijack a commercial airliner and crash it into a building on U.S. soil, a plot DOJ describes as an attempt to replicate the September 11 attacks.

Fit/Limitations: Confirmed, adjudicated, primary DOJ source, and directly on-point for TSA's named "hijacking / aircraft used as weapons" category. Plot was disrupted before any operational attempt reached an aircraft or airport.
Source: https://www.justice.gov/opa/pr/cholo-abdi-abdullah-sentenced-life-prison-conspiring-commit-911-style-terrorist-attack-0

Sources

- DOJ — Cholo Abdi Abdullah sentencing (al-Shabaab hijacking plot)
- https://www.wisn.com/article/passenger-arrested-after-hijack-scare-forces-emergency-landing-in-madison/71451242

VI. Insider Threats

TSA's 2020 Insider Threat Roadmap defines this risk precisely because credentialed access bypasses the standard screening systems entirely. A badge, uniform, or cockpit jump-seat privilege substitutes for the scrutiny a commercial traveler would face. TSA's 2026-2030 strategy elevates this from roadmap language to a named strategic objective, explicitly titling Objective 2.2 "Address Insider Threats" and naming Employee and Credentialed Population Vetting as a key activity across the sector.

The case record spans several distinct forms of access. A former TSA officer at LAX was sentenced to 70 months in federal prison for using his unscreened access to deliver what he believed was methamphetamine past the secure-side checkpoint in exchange for cash. At Washington Dulles, an airport services worker holding a Special Access Seal pleaded guilty to importing cocaine and counterfeit currency discovered in his cargo bag. In January 2025, ICE's Homeland Security Investigations arm arrested twelve individuals across two separate drug-smuggling operations run out of U.S. airports by airline employees. The 2018 Sea-Tac "Sky King" incident, in which a properly credentialed ground service employee stole an unoccupied aircraft and crashed it after a brief flight, illustrates a different facet of the same category. And the 2007 JFK fuel-tank bomb plot, discussed in Section III, involved a former airport employee whose insider knowledge of the site enabled surveillance and target selection.

A distinct subcategory of threat involves flight crew rather than ground-side employees. Airline crew members holding Known Crewmember (KCM) status are permitted to bypass standard passenger screening lanes, a program designed to reduce redundant screening for personnel already subject to background vetting. The 2023 case of off-duty Alaska Airlines pilot Joseph Emerson attempted to activate the fire-suppression system to shut down both engines mid-flight while riding in the cockpit jump seat on Horizon Flight 2059 demonstrates additional exploitable threat landscapes.

Incident Detail

Dulles Airport Services Worker, Cocaine and Counterfeit Currency Importation (2025)
A Dulles airport services worker holding a Special Access Seal pleaded guilty to importing cocaine and counterfeit currency discovered in his cargo bag.

Fit/Limitations: Confirmed, adjudicated (guilty plea), primary DOJ source. Also cross-referenced in Section X.B (Drug Smuggling), since this case sits at the intersection of insider access and narcotics trafficking.
Source: https://www.justice.gov/usao-edva/pr/airport-services-worker-dulles-international-airport-pleads-guilty-smuggling-cocaine

Airline Employee Drug Smuggling Arrests (January 2025)
ICE's Homeland Security Investigations arm arrested twelve individuals across two separate drug-smuggling operations run out of U.S. airports by airline employees.

Fit/Limitations: Confirmed law enforcement action, primary ICE source. Demonstrates insider-enabled smuggling as an ongoing, multi-operation pattern rather than an isolated case. Also cross-referenced in Section X.B.
Source: https://www.ice.gov/news/releases/ice-arrests-airline-employees-involvement-international-drug-smuggling

Off-Duty Pilot Joseph Emerson, Alaska Horizon Flight 2059 (2023)
An off-duty Alaska Airlines pilot riding in the cockpit jump seat attempted to activate the fire-suppression system to shut down both engines mid-flight; later attributed to psychedelic mushroom use.

Fit/Limitations: Confirmed, charged case (83 counts of attempted murder and endangerment). Distinct sub-vector from the others, demonstrates credentialed cockpit access as an exploitable vector absent criminal intent to smuggle or attack.
Source: https://www.nbcnews.com/news/us-news/man-charged-attempted-murder-trying-shut-alaska-airlines-engines-fligh-rcna121681

Former TSA Officer, LAX Methamphetamine Smuggling (2022)
A former TSA officer was sentenced to 70 months in federal prison for using his unscreened access to deliver what he believed was methamphetamine past the secure-side checkpoint on two occasions, in exchange for cash

Fit/Limitations: Confirmed, adjudicated case. Particularly sharp example since the individual responsible for screening others was himself the exploited vector, directly illustrates why credentialed access bypasses the system it's meant to protect.
Source: https://www.cbsnews.com/losangeles/news/tsa-employee-sentenced-for-drug-smuggling-at-lax/

TSA Insider Threat Roadmap (2020)
TSA's governing framework defining insider threat as an individual with authorized access who wittingly or unwittingly misuses, or allows others to misuse, that access, manifesting as sabotage, smuggling, espionage, or unauthorized access to security-restricted areas and information.

Fit/Limitations: Not an incident, the foundational policy document. Confirms insider threat as a distinct, named TSA priority rather than a subset of another category.
Source: https://www.tsa.gov/sites/default/files/insider_threat_roadmap.pdf

Sea-Tac "Sky King" Incident (2018)
A properly credentialed ground service employee stole an unoccupied aircraft and crashed it after a brief flight; the FBI's investigation concluded he had legitimate access in the ordinary course of his duties and did not violate any existing security protocol before the theft occurred.

Fit/Limitations: Confirmed, primary FBI source. Distinct from the other cases, illustrates insider risk as a function of legitimate access itself rather than a vetting or screening failure, since no protocol

was actually broken until the moment of the theft.
Source: https://www.fbi.gov/contact-us/field-offices/seattle/news/press-releases/fbi-completes-investigation-into-august-2018-unauthorized-flight-from-seattle-tacoma-airport

JFK Airport Fuel-Tank Bomb Plot (2007)
A former airport employee among the conspirators used his knowledge of the site to conduct surveillance and identify targets and escape routes.

Fit/Limitations: Cross-referenced from Section III. Confirmed case; illustrates the IED and insider-threat categories intersecting directly, insider knowledge enabling target selection rather than direct physical access enabling smuggling.
Source: https://www.aljazeera.com/news/2007/6/3/us-foils-plot-to-bomb-airport

Sources

- TSA Insider Threat Roadmap (2020)
- CBS News — TSA officer sentenced for drug smuggling at LAX
- DOJ, Eastern District of VA — Dulles airport services worker cocaine plea
- ICE — airline employee drug smuggling arrests (Jan 2025)
- FBI Seattle — Sky King investigation closure
- Al Jazeera — JFK Airport fuel-tank bomb plot (2007)
- NBC News — off-duty Alaska Airlines pilot Joseph Emerson charged
- PBS News — Joseph Emerson sentencing

VII. Unmanned Aircraft Systems

TSA names UAS interference with airport operations as a standing aviation risk, and the sector-wide strategy separately flags UAS as difficult to detect, launchable from nearly any location, and capable of standoff delivery of explosives or CBRN agents, surveillance, or cyber intrusion. The clearest and most severe domestic case to date is the June 2026 plot to attack the UFC Freedom 250 event on the White House South Lawn, held to mark America's 250th anniversary, using explosive-laden drones. The FBI disrupted the plot on June 10, 2026, days before the event, after a tip from one suspect's own mother; five men were charged across four federal districts (Ohio, Missouri, Nebraska, and California) with conspiring to deploy drones armed with explosives to force a mass evacuation, followed by a planned second wave in which snipers would fire on the fleeing crowd, and a further wave targeting a security checkpoint. While not an airport-specific case, it is the single most consequential confirmed U.S. UAS threat in this report, a coordinated, multi-state, explosive-drone mass-casualty plot against a major public event, disrupted through investigative work rather than technical detection. It underscores that the drone threat named in TSA's strategy extends beyond airspace incursions at airports to any large, open, aviation-adjacent gathering.

Several additional recent cases illustrate the range and growing frequency of this threat specifically at airports. In February 2026, the FAA halted all flights at El Paso International Airport for roughly ten days after a drone incursion that the U.S. Transportation Secretary attributed to a Mexican drug cartel. Pentagon officials noted that more than 1,000 incidents occur monthly along the U.S.-Mexico border, most without crossing into U.S. airspace. This case is discussed further in Section X, since cartel-operated drones function simultaneously as an airspace-incursion threat and as smuggling/surveillance infrastructure.

In June 2026, a JetBlue pilot reported a mid-air collision with a drone while on approach to JFK Airport at roughly 3,000 feet. The FAA opened an investigation. A post-landing inspection found no damage to the aircraft. Also in 2026, the FAA issued a ground stop at Newark Liberty International Airport after two drones were sighted at 3,500 feet near neighboring Teterboro Airport. In late 2024 and early 2025, a drone sighted near air traffic near Harry Reid International Airport in Las Vegas prompted a temporary runway disruption.

The FAA's own Q2 2026 quarterly report found 601 drone sightings reported near U.S. airports between April and June 2026, nearly doubling the 320 in the prior quarter. The agency notes more than 100 monthly reports as an ongoing baseline.

The Global Drone Threat Is Accelerating Faster Than Airport Defenses

The U.S. cases in this section sit inside a global trendline of drone warfare advancing faster than most civil aviation systems are built to counter, even when the fighting itself is thousands of miles away.

On May 4, 2025, a Houthi ballistic missile struck the grounds of Ben Gurion Airport in Tel Aviv, the first time Houthi fire had ever landed at a major international airport. The impact injured six people, briefly halted all flight operations, and prompted most foreign carriers to suspend service to Israel for

days. The disruption reached U.S. airports directly. Flights to Newark and JFK were delayed roughly 90 minutes as airlines rerouted around the closure. Israel's own air defense system attempted, and failed, to intercept the missile.

That failure is not an isolated data point. Ukraine is now producing an estimated 4 to 7 million drones annually, roughly seventy times total U.S. combat drone output. The Ukrainian drone industry has pioneered autonomous swarm coordination, AI-guided targeting, and fiber-optic drones immune to jamming, developed and iterated on timelines of weeks rather than the years typical of conventional defense acquisition. Iran's drone technology has already posed direct operational challenges for U.S. and Gulf-state militaries. None of this technology is contained to its theater of origin; commercial and quasi-military drone capability proliferates quickly once demonstrated at scale.

The throughline for this report: the same category of threat TSA names as "difficult to detect, launchable from nearly any location" is being actively developed, tested, and iterated against real air-defense systems overseas, at a pace considerably faster than the counter-drone architecture protecting U.S. commercial airports. The FAA's own Q2 2026 data suggests U.S. airports are already feeling the leading edge of that gap.

Incident Detail

UFC Freedom 250 Explosive-Drone and Sniper Plot (Disrupted June 10, 2026)

Five men were charged in a multi-state plot to deploy explosive-laden drones against the UFC Freedom 250 event at the White House, intended to force a mass evacuation into a planned sniper ambush, with a further wave targeting a security checkpoint. The plot was disrupted after a suspect's mother alerted local police to his online communications and firearms purchases.

Fit/Limitations: Primary DOJ source, confirmed federal charges (conspiracy, attempted murder of a federal officer). The most severe UAS-related plot in this report by consequence, though not airport-specific. Investigation remains ongoing as of the source date; full prosecution outcomes not yet available.
Source: https://www.justice.gov/opa/pr/five-men-arrested-and-charged-plot-attack-and-kill-government-officials-and-others-attending

El Paso International Airport, Cartel Drone Incursion (February 2026)

The FAA halted all flights at El Paso International Airport for approximately ten days after a drone incursion the U.S. Transportation Secretary attributed to a Mexican drug cartel.

Fit/Limitations: Confirmed government action (FAA flight halt), though the cartel attribution rests on a public statement from the Transportation Secretary rather than a published investigative finding.
Source: https://www.usnews.com/news/top-news/articles/2026-02-11/us-halts-all-flights-at-texass-el-paso-airport-for-10-days

El Paso Airspace Shutdown, Context and Analysis

Additional reporting on the El Paso shutdown, including Pentagon officials' note that more than

1,000 drone incidents occur monthly along the U.S.-Mexico border, most without crossing into U.S. airspace.

Fit/Limitations: Secondary reporting providing scale context for the border drone environment; useful for showing the El Paso incident is not isolated, but the 1,000/month figure describes border activity broadly, not confirmed airport-specific incursions.
Source: https://www.aljazeera.com/news/2026/2/12/why-was-el-paso-airspace-shut-down-drones-security-fears-and-confusion

JetBlue Drone Collision, JFK Airport (June 2026)
A JetBlue pilot reported a mid-air collision with a drone while on approach to JFK at roughly 3,000 feet; the FAA opened an investigation, and a post-landing inspection found no damage.

Fit/Limitations: Confirmed collision report under FAA investigation, but no confirmed drone operator or intent identified, could reflect reckless/negligent operation rather than malicious targeting. No damage found limits severity as a case example.
Source: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/june/drone-jetblue-jfk-collision-droneshield-2026-report/

Newark Liberty International Airport, Drone Ground Stop
The FAA issued a ground stop after two drones were sighted at 3,500 feet near neighboring Teterboro Airport; normal operations resumed after roughly an hour.

Fit/Limitations: Confirmed FAA action at a major East Coast hub; brief duration and no confirmed operator identified limit severity, but adds a fourth distinct airport-specific U.S. case.
Source: https://gulfnews.com/business/aviation/drone-sightings-briefly-disrupt-flights-at-newark-airport-in-us-but-operations-are-now-back-to-normal-1.1548227576512

Harry Reid International Airport, Drone Runway Disruption (Late 2024/Early 2025)
A drone sighted in close proximity to air traffic near Harry Reid International Airport prompted a temporary runway disruption.

Fit/Limitations: Secondary/trade press reporting rather than a primary FAA or DOJ source; demonstrates recurrence of runway-disruption pattern
Source: https://www.thetraveler.org/drone-threats-force-new-look-at-us-airport-security/

FAA Q2 2026 Drone Sightings Report, Nationwide Trend Data
The FAA's official Q2 2026 quarterly report found 601 drone sightings near U.S. airports between April and June 2026, compared with 320 in the prior quarter.

Fit/Limitations: Primary FAA statistical source; evidence the threat is scaling nationally rather than remaining anecdotal. No breakdown by intent (malicious vs. reckless/negligent operation) is provided in the underlying data.
Source: https://dronelife.com/2026/07/06/faa-drone-sightings-near-airports-second-quarter-2026/

International Drone Advances Sources

2025 Houthi Attack on Tel Aviv (Ben Gurion) Airport
A Houthi ballistic missile struck the grounds of Ben Gurion Airport on May 4, 2025, near the access road to Terminal 3, injuring eight people and halting air, road, and rail traffic; the first time Houthi fire had landed at a major international airport.

Fit/Limitations: Demonstrates threats outside United States aviation centers but represents global emergence of drone born attacks on ally infrastructure
Source: https://news.sky.com/story/netanyahu-vows-to-retaliate-against-houthis-and-iran-after-missile-attack-13361736

CBS News, Houthi Missile Launch Halts Flights at Ben Gurion Airport
Confirms the missile strike, injury count, and disruption to air, road, and rail traffic at Israel's main international airport.

Fit/Limitations: Demonstrates broad impact of attacks against aviation infrastructure at ally aviation centers
Source: https://www.cbsnews.com/news/ben-gurion-international-airport-israel-houthi-missile-launch/

All India Radio, Houthi Missile Strike Disrupts Ben Gurion Airport Operations
Confirms downstream flight delays to U.S.-bound carriers, including roughly 90-minute delays to flights bound for Newark and JFK.

Fit/Limitations: The primary incident was abroad but had downstream impacts on United States aviation scheduling and access to transportation
Source: https://www.newsonair.gov.in/missile-from-yemen-hits-near-ben-gurion-airport-6-injured-flights-resume

Council on Foreign Relations, How Ukraine's Drone Innovation Reversed Russia's Momentum
Details Ukraine's estimated 4-6 million annual drone production, autonomous swarm coordination, and rapid iteration cycles.

Fit/Limitations: Demonstrates the scale of global drone innovation and potential threat impacts to aviation centers, including the United States
Source: https://www.cfr.org/articles/how-ukraines-drone-innovation-reversed-russias-momentum

Modern War Institute, Transforming Acquisition for the Drone Age
Cites Ukraine's plan to produce over 7 million drones in 2026, roughly seventy times U.S. annual combat drone output.

Fit/Limitations: U.S. military-academic source (West Point)
Source: https://mwi.westpoint.edu/build-at-scale-innovate-at-the-edge-close-the-feedback-loop-fast-transforming-acquisition-for-the-drone-age/

Sources

- U.S. News — FAA halts all flights at El Paso airport for 10 days
- Al Jazeera — why El Paso airspace was shut down
- ASIS/Security Management — JetBlue drone collision at JFK (June 2026)
- The Traveler — Harry Reid International drone disruption
- DOJ — Five men arrested and charged in plot to attack UFC Freedom 250 with explosive drones and snipers (June 2026)
- U.S. News — FAA halts all flights at El Paso airport for 10 days
- Al Jazeera — why El Paso airspace was shut down
- ASIS/Security Management — JetBlue drone collision at JFK (June 2026)
- Gulf News — drone sightings briefly disrupt flights at Newark airport
- The Traveler — Harry Reid International drone disruption
- DroneLife — FAA data shows drone sightings near airports nearly doubled in Q2 2026
- Wikipedia — 2025 Houthi attack on Tel Aviv (Ben Gurion) airport
- CBS News — Houthi missile launch halts flights at Ben Gurion Airport
- All India Radio (newsonair.gov.in) — Houthi missile strike disrupts Ben Gurion Airport operations, U.S. flight delays
- Council on Foreign Relations — How Ukraine's Drone Innovation Reversed Russia's Momentum
- Modern War Institute — Transforming Acquisition for the Drone Age

VIII. Cybersecurity

Cybersecurity is elevated to its own standalone strategic goal in TSA's 2026-2030 strategy which demonstrated a shift from earlier strategic goals that treated cyber risk as part of other risk categories instead of its own.

The past 18 months of open-source reporting show this is not just a potential threat. On August 24, 2024, the Rhysida ransomware group breached Port of Seattle systems, disrupting baggage handling, check-in kiosks, ticketing, Wi-Fi, and passenger display boards at Seattle-Tacoma International Airport for weeks. The Port later confirmed roughly 90,000 people had personal information accessed in the breach. Officials later stated federal partner systems (FAA, TSA, CBP) and airline-proprietary systems were not affected.

On March 18, 2025, the hacktivist group Dark Storm Team claimed a DDoS attack against Los Angeles International Airport, flooding systems until flight information displays went dark, baggage handling stalled, and electronic check-in went offline across terminals. Ten days later, on March 28, 2025, Hartsfield-Jackson Atlanta International Airport confirmed a separate denial-of-service attack that briefly disrupted its public website. This attack did not affect flight operations, though.

In August 2025, Envoy Air was compromised by the Clop ransomware group through a zero-day vulnerability in Oracle's E-Business Suite platform. In October 2025, hackers gained access to Harrisburg International Airport's public address system and broadcast pro-Hamas messaging, causing panic among travelers.

Incident Detail

Harrisburg International Airport, PA System Hijacking (October 2025)
Hackers gained access to the airport's public address system and broadcast pro-Hamas messaging, causing panic among travelers.

Fit/Limitations: A hybrid case combining cyber intrusion with an information-operation objective, distinct from the ransomware/DDoS cases in this section. Sourced from trade press rather than a primary airport authority or FBI statement
Source: https://www.travelandtourworld.com/news/article/us-airports-under-siege-cyberattacks-target-travelers-stranding-thousands-whats-next-for-2026/

Envoy Air / Clop Ransomware, Oracle Zero-Day Exploit (August 2025)
Envoy Air, a regional subsidiary of American Airlines, was compromised by the Clop ransomware group through a zero-day vulnerability in Oracle's E-Business Suite platform.

Fit/Limitations: Confirmed incident tied to a named threat actor (Clop) and a specific, identifiable vulnerability.
Source: https://breached.company/american-airlines-subsidiary-hit-by-clop-ransomware-in-oracle-zero-day-attack/

Los Angeles International Airport, Dark Storm Team DDoS Attack (March 18, 2025)
The hacktivist group Dark Storm Team claimed a DDoS attack on LAX that took down flight information displays, baggage handling systems, and electronic check-in terminals

Fit/Limitations: Incident at LAX, with a named threat actor. Sourced from trade press citing cybersecurity research firm SOCRadar rather than a primary LAX/LAWA statement
Source: https://www.travelandtourworld.com/news/article/seattle-tacoma-joins-hartsfield-jackson-and-lax-airports-to-face-massive-cyberattacks-where-thousands-of-passengers-were-stranded-giving-surge-to-travel-chaos-is-your-future-air-travel-in-jeopardy/

Hartsfield-Jackson Atlanta International Airport, Denial-of-Service Attack (March 28, 2025)
ATL confirmed a denial-of-service attack that briefly disrupted its public website; airport officials told FOX 5 Atlanta the attack did not affect flight operations.

Fit/Limitations: A separate, distinct incident from the LAX case above, occurred ten days later and was confirmed directly by airport officials to local media. Attack was contained to the public website with no operational impact, making this a comparatively minor case relative to the others in this section.
Source: https://www.travelandtourworld.com/news/article/seattle-tacoma-joins-hartsfield-jackson-and-lax-airports-to-face-massive-cyberattacks-where-thousands-of-passengers-were-stranded-giving-surge-to-travel-chaos-is-your-future-air-travel-in-jeopardy/

Seattle-Tacoma International Airport, Rhysida Ransomware Attack (August 24, 2024)
The Rhysida ransomware group breached Port of Seattle systems, disrupting baggage handling, check-in kiosks, ticketing, Wi-Fi, passenger displays, and the Port's website; roughly 90,000 people had personal data accessed, though the Port stated federal and airline-proprietary systems were unaffected and it refused to pay the ransom demand.

Fit/Limitations: Port of Seattle disclosure. Named threat actor (Rhysida), confirmed impact scope, and an official public statement distinguishing what was and wasn't compromised.
Source: https://www.portseattle.org/news/port-cyberattack-archive

IX. Sabotage at Maintenance Facilities

Aircraft maintenance in the U.S. is a heavily regulated, credential-controlled environment. The FAA requires certified mechanics, documented inspection signoffs, and multiple quality-control checks before an aircraft returns to service. This structure is designed to catch the kind of tampering seen in the case below before an aircraft ever reaches a runway. The rarity of confirmed maintenance-facility sabotage cases reflects an effective inspection and sign-off process, not an indication that the underlying insider-access risk has gone away. This same distinction is drawn in Sections IV and V for standoff weapons and hijacking.

TSA names sabotage at maintenance facilities as a distinct aviation risk category. The clearest confirmed U.S. case is Abdul-Majeed Marouf Ahmed Alani, a former American Airlines mechanic who, in July 2019, glued a foam substance into the air data module of a Boeing 737 scheduled to carry 150 passengers from Miami to Nassau. Pilots aborted takeoff after an error alert. Alani later admitted he tampered with the aircraft hoping to generate overtime work amid a stalled union contract dispute and was sentenced to 37 months in federal prison. Prosecutors separately raised concerns about possible terrorism sympathies but did not pursue terrorism specific prosecution. This section rests on a single strong case rather than a broader pattern, and that limitation is stated directly: no second confirmed U.S. maintenance-facility sabotage case has been confirmed in recent years.

Incident Detail

Abdul-Majeed Marouf Ahmed Alani, American Airlines Maintenance Sabotage (July 2019)
A former American Airlines mechanic glued a foam substance into the air data module of a Boeing 737 scheduled to carry 150 passengers from Miami to Nassau. Pilots aborted takeoff after an error alert during pre-flight checks; Alani admitted he tampered with the aircraft hoping to generate overtime work amid a stalled union contract dispute and was sentenced to 37 months in federal prison.

Fit/Limitations: Primary DOJ source, confirmed and adjudicated. The only confirmed U.S. maintenance-facility sabotage case. Prosecutors raised, but did not formally charge, possible terrorism sympathies. The confirmed motive was financial/labor-dispute grievance, not ideological.
Source: https://www.justice.gov/usao-sdfl/pr/former-american-airlines-mechanic-sentenced-prison-attempting-destroy-aircraft

Sources

- DOJ, Southern District of FL — former American Airlines mechanic sentenced for attempting to destroy an aircraft

PART TWO: RISKS AROUND AVIATION

X. Transnational Crime Exploiting Aviation Infrastructure

TSA's National Strategy for Transportation Security is built to counter attacks on aviation infrastructure and the traveling public. The strategy is not designed to address counter-narcotics or anti-trafficking threats. This represents a reasonable scope boundary for the TSA's strategic plan. There is a gap in the general threat assessment. The same aviation infrastructure TSA secures against attack can also be exploited by transnational criminal organizations for different purposes. This section documents additional uses like human and child trafficking, drug smuggling, and bulk cash smuggling and cartel-operated drones.

X.A Human and Child Trafficking

Unlike currency and narcotics enforcement, human trafficking detection at airports is not a seizure-statistic exercise. Federal law enforcement agencies must be trained around behavioral red-flag indicators. A traveler who does not control their own travel documents. Someone who cannot answer basic questions about their destination independently. Mismatched responses between traveling companions. Hartsfield-Jackson Airport published an indicator framework ahead of the 2026 FIFA World Cup as part of a dedicated Atlanta trafficking crackdown on human and child trafficking. Dallas-Fort Worth Airport formalized a public pledge alongside other transportation-sector leaders to support trafficking-awareness efforts. Reporting for human and child trafficking at aviation centers does not include traditional stop or seizure metrics. Federal law enforcement at aviation centers also acts as deterrence for potential trafficking operations. This represents a sourcing gap rather than evidence the threat is smaller than the other categories in this report.

Incident Detail

Atlanta Hartsfield-Jackson, Trafficking Crackdown Ahead of FIFA World Cup (January 2026)
Atlanta expanded its published behavioral indicator framework and launched a dedicated trafficking crackdown at Hartsfield-Jackson ahead of the 2026 FIFA World Cup.

Fit/Limitations: The most developed public example of an indicator-based detection model in this section.
Source: https://www.fox5atlanta.com/news/atlanta-human-trafficking-crackdown-ahead-world-cup

Dallas-Fort Worth Airport, Human Trafficking Awareness Pledge
DFW Airport formalized a public pledge alongside other transportation-sector leaders to support trafficking-awareness training and reporting.

Fit/Limitations: A policy/commitment source rather than an incident. Shows institutional awareness and program existence but provides no case-level or statistical evidence of trafficking activity or interdictions at DFW specifically.

Source: https://www.dfwairport.com/dfwnewsroom/archivednews/dfw-airport-joins-transportation-leaders-in-pledging-to-help-fight-human-trafficking/

X.B Drug Smuggling

A 22-year-old traveler was arrested at Hartsfield-Jackson with approximately $2.9 million in narcotics bound for São Paulo. The 2026 Atlanta-Carolinas HIDTA Threat Assessment identifies methamphetamine as the top regional drug threat, with cocaine trafficking patterns varying by demographic and sub-region. Insider-facilitated cases, discussed in full in Section VI, are directly relevant here as well. The former TSA officer who used unscreened access to smuggle narcotics through LAX, the Dulles airport services worker convicted of importing cocaine, and the twelve airline employees arrested in January 2025 across two separate airport-based smuggling operations all demonstrate that drug smuggling through aviation infrastructure is frequently insider-enabled rather than purely a passenger-screening challenge.

Incident Detail

Hartsfield-Jackson Atlanta, $2.9M Narcotics Seizure
A 22-year-old traveler was arrested at Hartsfield-Jackson with approximately $2.9 million in narcotics (THC wax, hashish, marijuana) bound for São Paulo.

Fit/Limitations: Confirmed arrest reported via national news
Source: https://www.usatoday.com/story/travel/news/2025/07/14/narcotics-seized-luggage-atlanta-airport/85195378007/?tbref=hp

Atlanta-Carolinas HIDTA 2026 Drug Threat Assessment
The regional threat assessment identifies methamphetamine as the top regional drug threat, with cocaine trafficking patterns varying by demographic and sub-region.

Fit/Limitations: Primary government regional assessment. Provides regional trend context rather than aviation-specific case data
Source:https://addictioncenterofexcellence.sc.gov/sites/daodas/files/users/user266/HIDTA%202026%20Threat%20Assessment%20-%20Final.pdf

Cross-Referenced Insider-Facilitated Cases (see Section VI for full detail)
The former TSA officer who used unscreened access to smuggle narcotics through LAX, the Dulles airport services worker convicted of importing cocaine, and the twelve airline employees arrested in January 2025 across two separate airport-based smuggling operations.

Fit/Limitations: Not re-sourced here, full citations and case detail live in Section VI (Insider Threats). Cross-referenced to demonstrate that drug smuggling through aviation infrastructure is frequently insider-enabled rather than purely a passenger-screening challenge.

X.C Illicit Cash / Bulk Currency Smuggling

U.S. law requires travelers to declare more than $10,000 in currency or monetary instruments leaving the country via a FinCEN 105 form. At Hartsfield-Jackson Atlanta, CBP seized more than $372,000 from two dozen travelers in the first quarter of 2026 alone. At Washington Dulles, CBP seized close to $100,000 from travelers over Memorial Day weekend 2026, including cash concealed by stitching it into clothing. At Fort Lauderdale-Hollywood, a traveler bound for Kingston, Jamaica was arrested on money laundering charges after CBP seized $53,800 in undeclared currency.

Incident Detail

CBP Atlanta, $372,264 Seized from 24 Travelers (Q1 2026)
CBP seized more than $372,000 in unreported currency from two dozen travelers at Hartsfield-Jackson in the first quarter of 2026.

Fit/Limitations: Primary CBP source, confirmed enforcement data.
Source: https://www.cbp.gov/newsroom/local-media-release/cbp-atlanta-officers-seize-over-372000-unreported-currency-atlanta

CBP Dulles, Nearly $100K Seized, Memorial Day Weekend 2026
CBP seized close to $100,000 from travelers at Dulles over Memorial Day weekend 2026, including cash concealed by stitching it into clothing.

Fit/Limitations: Local news reporting on a CBP enforcement action; concealment method (stitched into clothing) signals premeditation rather than inadvertent reporting failure.
Source: https://wtop.com/dc/2026/06/hidden-in-underwear-cbp-seizes-nearly-100k-from-dulles-travelers/

CBP Fort Lauderdale, $53,800 Seizure, Money Laundering Arrest
A traveler bound for Kingston, Jamaica was arrested on money laundering charges after CBP seized $53,800 in undeclared currency.

Fit/Limitations: Primary CBP source, confirmed enforcement action with an associated criminal charge, distinguishing this from a civil seizure alone.
Source: https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-53800-undeclared-currency-fort-lauderdale-airport

X.D Cartel Drone Use

The February 2026 El Paso airspace shutdown, discussed in Section VII as a UAS incident, belongs in this threat assessment, as well. Pentagon officials describe the drones involved as cartel-operated, used both for surveillance of border patrol movements and for drug smuggling activity. This is the clearest example in this report of a threat that is simultaneously a risk to aviation and an actor exploiting vulnerabilities in the aviation sector. The purpose of the drone activity is transnational narcotics logistics rather than an attack on the airport itself.

Incident Detail

El Paso International Airport, Cartel Drone Incursion (February 2026)
The FAA halted all flights at El Paso International Airport for approximately ten days after a drone incursion the U.S. Transportation Secretary attributed to a Mexican drug cartel, used both for surveillance and drug smuggling activity.

Fit/Limitations: Cross-referenced from Section VII. Confirmed government action (FAA flight halt); cartel attribution rests on a public statement from the Transportation Secretary rather than a published investigative finding. The clearest example in this report of the Part One/Part Two convergence this report's Trend Analysis section argues for.
Source: https://www.usnews.com/news/top-news/articles/2026-02-11/us-halts-all-flights-at-texass-el-paso-airport-for-10-days

Sources

- FOX 5 Atlanta — trafficking crackdown ahead of FIFA World Cup (Jan 2026)
- DFW Airport — public pledge on human trafficking awareness
- Men's Journal / Yahoo — ATL $2.9M narcotics seizure
- Atlanta-Carolinas HIDTA 2026 Drug Threat Assessment
- CBP Atlanta — $372,264 seized from 24 travelers, Q1 2026
- WTOP — nearly $100K seized at Dulles, Memorial Day 2026
- CBP — Fort Lauderdale $53,800 seizure, money laundering arrest
- U.S. News — El Paso airport flight halt, cartel drone incursion

XI. OSINT-Reported Incidents, Unverified and Non-Credible Threats

This section contains a distinct purpose from Parts One and Two. Every case in the prior sections is either a DOJ prosecution, a TSA/CBP enforcement action, or a government-published threat assessment. The cases below are media-reported security responses to threats later assessed as non-credible. They are included because a methodology built on open-source intelligence should account for reporting volume and institutional response, not only adjudicated outcomes. The law enforcement and security response to suspected incidents reflect the operating assumption that a reported threat must be treated as real until affirmatively ruled out, since the cost of a false negative in aviation security is substantially higher than the cost of a false positive. None of the below resulted in a confirmed device, weapon, or credible actor being identified. Media reported incidents in this section were independently tracked by Grayline Intelligence as part of its ongoing OSINT monitoring.

Incident Detail

United Flight 2408, Lands Safely at Dulles After Bomb Threat
200 passengers and seven crew were deplaned via airstairs at Denver International Airport after a reported bomb threat; the aircraft was fully swept, no explosives were found, and the flight departed more than five hours late.

Fit/Limitations: No confirmed device found, assessed as non-credible but demonstrates law enforcement response to aviation threats
Source: https://www.nbcwashington.com/news/local/flight-from-denver-lands-safely-at-dulles-airport-after-bomb-threat/4093085/

Frontier Flight 2539, Verbal Bomb Threat, Hartsfield-Jackson (March 29, 2026)
A passenger made a verbal bomb threat as the aircraft taxied to the gate; the FBI determined the threat was not credible, and Atlanta police treated it as an unruly-passenger incident rather than a hijacking or bomb threat.

Fit/Limitations: Local news reporting; law enforcement's own "unruly passenger" characterization is itself evidence the incident was downgraded from an initial security response to a lesser classification after investigation.
Source: https://www.fox5atlanta.com/news/police-investigate-bomb-threat-frontier-flight-atlanta-airport

Kansas City International Airport, Terminal and Parking Garage Threat (March 8, 2026)
A call reporting a possible device inside the terminal and parking garage triggered a full terminal evacuation and a two-hour ground stop, producing 169 flight delays and two cancellations before FBI Director Kash Patel publicly confirmed the threat was not credible.

Fit/Limitations: Local news source; confirmation of non-credibility came from a named federal official (FBI Director). Highest operational cost of the incidents listed here, 169 delays and 2 cancellations from a single phoned-in report.

Source: https://www.kctv5.com/2026/03/08/passengers-evacuated-kci-after-possible-threat-fbi-investigating/

Southwest Flight 2094, Diversion to Atlanta, Tactical Response (March 6, 2026)
The flight, en route from Nashville to Fort Lauderdale, diverted to Atlanta after a mid-flight passenger disturbance; armed tactical units boarded the aircraft before the FBI and Atlanta Police Department determined there was no credible threat.

Fit/Limitations: The response (armed tactical boarding) was disproportionate to the confirmed cause.
Source: https://www.foxbusiness.com/lifestyle/southwest-flight-diverts-atlanta-airport-armed-tactical-units-detain-man-frightening-security-scare

Detroit Metro Airport, Hoax Bomb Threat Arrest (June 2025)
A Michigan man called Spirit Airlines and described a fabricated bomb threat against a Detroit-to-Los Angeles flight, triggering a full cancellation and K9 sweep before his arrest.

Fit/Limitations: Primary DOJ source. The only case in this section with a confirmed criminal prosecution (for the hoax call itself) rather than an unresolved or uncharged incident.
Source: https://www.justice.gov/usao-edmi/pr/monroe-michigan-man-arrested-calling-hoax-bomb-threat-flight-detroit-metro-airport

LaGuardia Airport, Shoulder-Fired Missile Security Bulletin (2026)
Air traffic controllers passed a security bulletin to arriving aircraft warning of a possible shoulder-fired missile threat near the airport.

Fit/Limitations: Precautionary and unconfirmed, no device or individual was ever verified. Trade press source (AeroXplorer) rather than a primary FAA or law enforcement statement
Source: https://aeroxplorer.com/articles/laguardia-tower-alerts-pilots-to-possible-shoulderfired-missile-threat-near-airport

Grayline Intelligence Tracker, Corroborating Source
Grayline's OSINT tracker independently logs incidents in this section as part of its ongoing monitoring of geopolitical threat reporting.

Fit/Limitations: Owned platform; included as a corroborating source for the section rather than a distinct incident. Confidence-scored per Grayline's own methodology rather than independently adjudicated.
Source: https://graylineintel.com

XIII. Legislative Landscape

Congress is currently considering multiple bills related to aviation security. Not every bill is attempting to solve the same challenges. The legislative landscape suggests lawmakers are aware of security gaps TSA has raised and are actively working to address them. The Safer Skies Act of 2025 is the most direct attempt to tighten security and standardize it across all methods of commercial aviation, independent of the class of aircraft, number of passengers, or terminal of departure.

H.R.2353, Safer Skies Act of 2025

This bill directs TSA to require that certain small public charter air carrier operations comply with AOSSP rather than the lighter TFSSP standard for public charter airlines with smaller planes and fewer passengers. It was introduced by Rep. Nick Langworthy (R-NY) on March 26, 2025 with 33 original bipartisan cosponsors. As of August 2026, it remains pending in the House Subcommittee on Transportation and Maritime Security. H.R.2353 is not the same bill as S.3481, the counter-UAS SAFER SKIES Act, discussed below. That bill was signed into law on December 18, 2025 as part of the FY2026 NDAA.

This bill has the potential to directly impact aviation security in the United States. The impact varies from threat to threat but provides direct solutions to known issues in aviation infrastructure.

Improvised Explosive Devices & Mass Casualty / Landside Attacks

AOSSP-level screening at FBO and charter terminals would close a specific unscreened entry point at aviation infrastructure. TFSSP screening may not be comprehensive enough to detect devices and weapons the same level that full AOSSP does. This change would not impact all landside or open-area vulnerability, nor is it designed to. The bill focuses on traveler screening; risks outside the scope of screening are not addressed.

Standoff Weapons Attack

This bill addresses passenger and baggage screening at the point of boarding. It does not impact perimeter or standoff threats that originate outside airport property, nor is it designed to.

Hijacking

Extending AOSSP screening to charter operations and FBO terminals would apply the same passenger vetting and weapons detection standard used to disrupt cases like the Abdullah plot. This bill would close a vulnerability tier where a hijacker could otherwise board a commercial aircraft with less scrutiny than at traditional airport terminals.

Insider Threats

There is a limited direct impact to insider threats. Insider risk stems from credentialed employees and crew access rather than passenger screening tier, so this bill would not change the underlying vulnerability documented in Section VI. Although, heightened facility-level security requirements under AOSSP could incidentally tighten access controls at charter terminals.

Unmanned Aircraft Systems

This bill governs passenger and baggage screening, not airspace or perimeter drone detection. There would be minimal impact on UAS threats. Increased screening and security at FBO terminals could act as a deterrence on potential threats, though.

Cybersecurity

This bill does not impact technology infrastructure.

Sabotage at Maintenance Facilities

Maintenance facility access and mechanic credentialing exist outside the passenger screening framework this bill amends. There would be no meaningful impact to this threat. Historical incidents suggest current security measures are effective.

Human & Child Trafficking

Charter terminals currently lack the trained-observer indicator programs used at major commercial hubs like Hartsfield-Jackson. AOSSP-level standards could extend comparable behavioral-detection training and protocols to a channel traffickers may otherwise treat as lower-scrutiny.

Illicit Cash and Bulk Currency Smuggling

Extending AOSSP standards to charter carriers would reduce the relative attractiveness of that channel for bulk cash movement. Although, CBP's currency-reporting enforcement operates independently of which TSA security tier a flight departs under.

The Safer Skies Act of 2025 has a direct and narrow goal: standardize security processes for all commercial passengers, independent of airline, aircraft class, passenger count, or terminal of departure. It is not designed to address every vector of aviation security, and the analysis above treats that limitation as a feature of honest scoping rather than a shortcoming. Within that scope, however, the bill would have a direct and measurable impact on several of the threats documented in this report, IEDs, hijacking, human and child trafficking, and illicit cash and bulk currency smuggling, by closing the specific screening-tier gap those threats have been shown to exploit.

Sources, H.R.2353

- Congress.gov — H.R.2353 (Safer Skies Act of 2025) summary: https://www.congress.gov/bill/119th-congress/house-bill/2353

- Congress.gov — H.R.2353 bill text (PDF): https://www.congress.gov/119/bills/hr2353/BILLS-119hr2353ih.pdf
- GovTrack — H.R.2353 status: https://www.govtrack.us/congress/bills/119/hr2353
- ALPA — 2026 legislative agenda: https://www.alpa.org/articles/2026/08/us-legislative-issues-on-alpas-pilot-partisan-agenda

S.3481, Counter-UAS SAFER SKIES Act (Distinct, Enacted Bill)

S.3481 addresses counter-unmanned aircraft system authority. It is named here to make the distinction from H.R.2353 explicit. Despite the nearly identical popular name, S.3481 was signed into law on December 18, 2025 as part of the FY2026 NDAA and addresses drone-related threats, not the charter-carrier screening gap H.R.2353 targets.

Sources — S.3481

- Federal Register — S.3481 counter-UAS rule (distinct, enacted bill): https://www.federalregister.gov/documents/2026/07/06/2026-13609/counter-uas-authority-for-state-local-tribal-and-territorial-law-enforcement-and-correctional

H.R.8770, SAFEGUARDS Act of 2026

On July 13, 2026, the House passed a package of ten bipartisan Homeland Security Committee bills addressing TSA modernization, three of which bear directly on the threat categories in this report. H.R.8770 redirects a portion of the passenger security fee into a dedicated Aviation Security Capital Fund, earmarking the first $500 million collected each fiscal year for checked-baggage explosives detection equipment and checkpoint technology.

Sources — H.R.8770

- House Homeland Security Committee — 10-bill TSA modernization package (Jul 2026): https://homeland.house.gov/2026/07/13/house-passes-10-homeland-security-bills-to-modernize-tsa-reform-ia-combat-terror-threats/
- Congress.gov — H.R.8770 (SAFEGUARDS Act of 2026): https://www.congress.gov/bill/119th-congress/house-bill/8770

H.R.9391, Reimbursable Screening Services Program (RSSP) Extension Act of 2026

Also part of the July 13, 2026 package, H.R.9391 expands the pilot program letting airports pay for additional TSA screening capacity.

Sources — H.R.9391

- House Homeland Security Committee — 10-bill TSA modernization package (Jul 2026): https://homeland.house.gov/2026/07/13/house-passes-10-homeland-security-bills-to-modernize-tsa-reform-ia-combat-terror-threats/
- Congress.gov — H.R.9391 (RSSP Extension Act of 2026): https://www.congress.gov/bill/119th-congress/house-bill/9391

H.R.9388, One-Stop Pilot Program Extension Act

H.R.9388 extends a program to allow international travelers skip re-screening on a connecting domestic flight if their foreign last-point-of-departure airport meets TSA-verified standards.

Sources — H.R.9388

- House Homeland Security Committee — 10-bill TSA modernization package (Jul 2026): https://homeland.house.gov/2026/07/13/house-passes-10-homeland-security-bills-to-modernize-tsa-reform-ia-combat-terror-threats/
- Congress.gov — H.R.9388 (One-Stop Pilot Program Extension Act): https://www.congress.gov/bill/119th-congress/house-bill/9388

S.1180 — Abolish TSA Act

Not every active bill intends to expand TSA's authority or security goals. S.1180 would dissolve TSA's screening function entirely and has seen no committee action since its 2025 introduction. Its practical prospects are limited, but its existence demonstrates that the legislative debate over aviation security architecture is contested rather than settled.

Sources — S.1180

- Congress.gov — S.1180 (Abolish TSA Act of 2025): https://www.congress.gov/bill/119th-congress/senate-bill/1180

Sources

- eCFR — 49 CFR Part 1544 (regulatory text)
- TSA — Aviation Programs (official AOSSP/TFSSP/PCSSP definitions)
- GAO-22-105063 — Aviation Security Programs review
- Federal Register — 2008 rulemaking (TSA's own gap acknowledgment)
- Eckert Seamans — TFSSP change / SkyWest trigger
- NBAA — Twelve-Five Standard Security Program (TFSSP)
- NBAA — Private Charter Standard Security Program (PCSSP)
- HSToday / OCCRP — aviation regulatory blind spot investigation
- BlackJet / Altitude Blog — current (2026) JSX screening description
- Congress.gov — H.R.2353 (Safer Skies Act of 2025) summary

- Congress.gov — H.R.2353 bill text (PDF)
- GovTrack — H.R.2353 status
- ALPA — 2026 legislative agenda
- Federal Register — S.3481 counter-UAS rule (distinct, enacted bill)
- House Homeland Security Committee — 10-bill TSA modernization package (Jul 2026)
- Congress.gov — H.R.8770 (SAFEGUARDS Act of 2026)
- Congress.gov — H.R.9391 (RSSP Extension Act of 2026)
- Congress.gov — H.R.9388 (One-Stop Pilot Program Extension Act)

XV. Author Biography

Austin Higgins serves as Chief Financial Officer of the Special Operations Association of America, where he supports the organization's national security, policy, and research initiatives. His open-source intelligence work focuses on global risk, emerging threats, and the use of publicly available information to support national security decision-making.

Higgins previously worked in management consulting, including engagements within the aviation industry, and later led product and risk initiatives focused on global commercial and geopolitical risk. His national security work has included supporting civilian evacuation operations in conflict zones, critical infrastructure and supply-chain research, and assessments of emerging and gray-zone threats.

Higgins is a former US Air Force linguist and a co-founder of the Global Counterterrorism and Threat Intelligence Research Institute at the University of Texas at Dallas, where he previously served as a lecturer.

XVI. Sourcing Appendix

Full citation list, consolidated below for quick reference.

- ODNI — 2025 Annual Threat Assessment
- HSToday — summary of ODNI 2025 ATA
- Al Jazeera — JFK Airport fuel-tank bomb plot (2007)
- CNN — thwarted Hartsfield-Jackson attack (Oct 2025)
- Osprey Flight Solutions — U.S. airport criminality case study
- DOJ — Fort Lauderdale shooting sentencing
- DOJ — LAX 2013 shooting sentencing
- Wikipedia — 2002 LAX El Al shooting
- Grayline Intelligence tracker
- Baltimore Sun — Lakhani sting operation affidavit
- Redorbit — Hemant Lakhani sentenced to 47 years
- FBI — criminal complaint filing, Hemant Lakhani
- Congress.gov / CRS — R48543, Funding Aviation Security and TSA Screening Functions
- GAO-04-728 — Aviation Security perimeter/access control review
- DOJ — Cholo Abdi Abdullah sentencing (al-Shabaab hijacking plot)
- TSA Insider Threat Roadmap (2020)
- CBS News — TSA officer sentenced, LAX drug smuggling
- DOJ EDVA — Dulles airport services worker cocaine plea
- ICE — airline employee drug smuggling arrests
- FBI Seattle — Sky King investigation closure
- NBC News — off-duty pilot Joseph Emerson charged
- PBS News — Joseph Emerson sentencing
- U.S. News — El Paso airport flight halt, cartel drone incursion
- Al Jazeera — why El Paso airspace was shut down
- ASIS/Security Management — JetBlue drone collision at JFK
- The Traveler — Harry Reid International drone disruption
- Aerospace Global News — 2025 aviation cyberattacks roundup
- Breached.Company — Envoy Air/Clop ransomware
- Travel and Tour World — Harrisburg PA system hijacking
- Web Asha Technologies — March 2025 DDoS on major U.S. airport
- PolySwarm — 2026 aviation cyber threat landscape
- DOJ SDFL — Miami mechanic sentenced for attempting to destroy an aircraft
- FOX 5 Atlanta — trafficking crackdown ahead of World Cup

- DFW Airport — human trafficking pledge
- Men's Journal / Yahoo — ATL $2.9M narcotics seizure
- Atlanta-Carolinas HIDTA 2026 Threat Assessment
- CBP Atlanta — $372,264 seized, Q1 2026
- WTOP — Dulles cash seizures, Memorial Day 2026
- CBP — Fort Lauderdale $53,800 seizure
- Hoodline — United Flight 2408 bomb threat at Denver
- NBC4 Washington — United Flight 2408 lands at Dulles
- FOX 5 Atlanta — Frontier Flight 2539 verbal bomb threat
- KCTV5 — Kansas City International Airport evacuation
- Fox Business — Southwest Flight 2094 diversion, tactical response
- CBS News Atlanta — Southwest Flight 2094, no credible threat
- DOJ, Eastern District of Michigan — Detroit Metro hoax bomb threat
- AeroXplorer — LaGuardia MANPADS security bulletin (2026)
- eCFR — 49 CFR Part 1544
- TSA — Aviation Programs (AOSSP/TFSSP/PCSSP)
- GAO-22-105063 — Aviation Security Programs review
- Federal Register — 2008 rulemaking (TSA gap acknowledgment)
- Eckert Seamans — TFSSP change / SkyWest trigger
- NBAA — TFSSP program page
- NBAA — PCSSP program page
- HSToday / OCCRP — aviation regulatory blind spot investigation
- BlackJet — 2026 JSX screening description
- Congress.gov — H.R.2353 summary
- Congress.gov — H.R.2353 bill text (PDF)
- GovTrack — H.R.2353 status
- ALPA — 2026 legislative agenda
- Federal Register — S.3481 counter-UAS rule (distinct bill)
- House Homeland Security Committee — 10-bill TSA modernization package
- Congress.gov — H.R.8770 (SAFEGUARDS Act of 2026)
- Congress.gov — H.R.9391 (RSSP Extension Act of 2026)
- Congress.gov — H.R.9388 (One-Stop Pilot Program Extension Act)
- Congress.gov — S.1180 (Abolish TSA Act of 2025)
- TSA — 6,678 firearms, 2024 annual total
- Forbes — 152% ten-year firearms increase
- TSA — San Antonio (SAT) partial-year 2025
- TSA — Wichita (ICT) partial-year 2025

- TSA — North Carolina partial-year 2025