MedCrave
Step into the World of Research
Aeronautics and Aerospace Open access Journal

Short communication

Open Access
CrossMark

Safeguarding U.S. airspace: an integrated safety, security, and operational resilience framework (IS2F) for business aviation in complex threat environments

Abstract

Business aviation within the United States operates under a highly sophisticated and mature safety ecosystem supported by rigorous regulatory oversight. However, the proliferation of asymmetrical threats—such as electronic warfare (GNSS interference), cyber vulnerabilities, and unauthorized airspace incursions—demands a paradigm shift. This paper introduces the Integrated Safety and Security Framework (IS2F), a novel methodology tailored to fortify U.S. business aviation against both operational hazards and unlawful interference. By synthesizing directives from the FAA, TSA, and ICAO, this research operationalizes proactive threat identification, layered defenses, and structured response mechanisms. The findings emphasize that protecting U.S. critical aviation infrastructure requires pilots to transcend traditional procedural discipline, acting as dynamic risk managers who actively defend national security interests.

Keywords: business aviation, flight safety, aviation security, operational resilience, GNSS interference, U.S. national security, critical infrastructure protection

Volume 10 Issue 2 - 2026

Gustavo Souza Kelly
Airline Transport Pilot (FAA/ANAC) Aviation Safety Specialist and Consultant, Brazil

Correspondence: Gustavo Souza Kelly, Airline Transport Pilot (FAA/ANAC) Aviation Safety Specialist and Consultant, Brazil

Received: March 26, 2026 | **Published:** April 13, 2026

Abbreviation: FAA, federal aviation administration; ICAO, international civil aviation organization; SMS, safety management system; IS2F, Integrated Safety and Security Framework; NORAD, north american aerospace defense command; NBAA, national business aviation association, ADIZ, air defense identification zones; USA, unmanned aircraft systems; RIS, raw inertial reference systems; ATC, air traffic control; ASRS, aviation safety reporting system

Introduction

Flight safety has traditionally been defined by the systematic mitigation of operational risks through standardized training, procedural adherence, and strict regulatory oversight. In the United States, this framework is championed by the Federal Aviation Administration (FAA) through its Safety Management System (SMS)[1] doctrine, which prioritizes hazard identification and risk mitigation. Concurrently, the International Civil Aviation Organization (ICAO)[2] reinforces that operational safety and aviation security (AVSEC) are deeply interdependent domains.

However, escalating geopolitical instability and asymmetrical conflicts have radically expanded the operational threat matrix. Modern business aviation is increasingly vulnerable to sophisticated external threats, including targeted GNSS disruption, cyber- physical attacks on avionics, and the weaponization of civilian airspace. Furthermore, the seamless integration of civil aviation within the U.S. national defense architecture— overseen by entities like the North American Aerospace Defense Command (NORAD)[3]—mandates uncompromising adherence to interception protocols and enhanced surveillance measures. To address these vulnerabilities, this study proposes a cohesive operational framework that directly aligns business aviation practices with broader U.S. national security objectives, ensuring the resilience of critical airspace infrastructure.

Methodology

This research adopts a qualitative, applied methodology grounded in a comprehensive analysis of modern aviation defense mechanisms.

The theoretical foundation is built upon:

a) Regulatory analysis of FAA operational guidance and SMS doctrine.

b) Review of ICAO safety and security frameworks.

c) Examination of TSA guidelines and industry best practices from the National Business Aviation Association (NBAA).

d) Integration of technical threat data from EUROCONTROL, the MITRE Corporation, and NASA.

This multidisciplinary approach emphasizes practical applicability, ensuring that theoretical frameworks translate directly into real-world operational resilience for flight crews.

The operational environment under conflict conditions

Armed conflict and geopolitical tensions fundamentally destabilize the predictability of civil flight operations. FAA guidance explicitly underscores the critical importance of flawless compliance with Temporary Flight Restrictions (TFRs) and Air Defense Identification Zones (ADIZ)[4]. In these highly regulated airspaces, strict adherence to identification, communication, and transponder protocols is not merely a safety requirement, but a matter of national defense.

[1]Federal Aviation Administration. Advisory Circular AC 120-92C – Safety Management Systems for Aviation Service Providers. FAA, 2023.
[2]International Civil Aviation Organization. Safety Management Manual (Doc 9859), 4th Edition, 2018; Annex 17 – Security, 2020.
[3]North American Aerospace Defense Command (NORAD). Aerospace Warning and Control Mission Overview. U.S. Department of Defense, 2020.
[4]Federal Aviation Administration. Aeronautical Information Manual (AIM). Sections on Temporary Flight Restrictions and Air Defense Identification Zones, FAA, 2023.

From a homeland security perspective, U.S. Department of Defense and NORAD procedures establish rigid interception protocols for any aircraft exhibiting non- compliant or anomalous trajectories. Consequently, minor procedural deviations— traditionally classified as benign operational errors—are increasingly interpreted as acute security threats. This convergence of safety and security results in:

1) A near-zero tolerance for procedural deviations.
2) Significantly increased cognitive and operational workload for flight crews.
3) Elevated, potentially catastrophic consequences for the misinterpretation of pilot intent by defense authorities.

Identification of suspicious and illicit activities

The early and accurate identification of operational anomalies is the cornerstone of modern aviation defense. TSA[5] guidelines emphasize that structured observation and objective verification are primary tools for preventing unlawful interference.

Pre-flight and ground indicators

Security vulnerabilities are often most pronounced before the aircraft leaves the tarmac. Indicators of elevated risk include inconsistencies in passenger identity, ambiguous travel purposes, and irregular cargo characteristics. TSA and FAA SMS guidelines mandate that these anomalies be evaluated systematically, integrating security risk assessments into standard pre-flight planning rather than relying on subjective judgment. Furthermore, inadequate perimeter control, irregular servicing activities, and the growing threat of unauthorized unmanned aircraft systems (UAS) near airports introduce severe collision and security risks.

In-flight indicators

In-flight anomalies often serve as the first indicators of covert external threats. Recent data from EUROCONTROL and MITRE regarding GNSS interference[6] demonstrates that electronic warfare attacks often manifest as subtle navigational inconsistencies rather than complete system failures.

To prevent escalation, pilots must be trained to immediately identify:

A. Discrepancies between GNSS data and raw Inertial Reference Systems (IRS).

B. Uncommanded or unexpected deviations in aircraft trajectory.

C. Anomalous or highly irregular Air Traffic Control (ATC) instructions that may indicate frequency spoofing.

Data from NASA's Aviation Safety Reporting System (ASRS)[7] confirms that early recognition of these subtle anomalies drastically reduces the likelihood of critical escalation.

Prevention and risk mitigation measures

Operational resilience requires the implementation of proactive, layered defenses across all phases of flight.

Pre-flight security integration: FAA SMS doctrine emphasizes that effective mitigation occurs prior to exposure. This requires rigorous verification of passenger identity, assessment of route proximity to restricted airspace, and the mandatory inclusion of security protocols in crew briefings. This establishes an impenetrable preventive barrier.

In-flight risk mitigation: Resilience relies on technological redundancy and disciplined execution. Adhering to FAA, ICAO, and RTCA[8] standards requires continuous cross-verification of navigation systems and strict cybersecurity practices to maintain the integrity of avionics.

Training and human factors: Human performance remains the ultimate failsafe.

Threat and Error Management (TEM) principles reinforce that highly trained, disciplined crews capable of complex decision-making under uncertainty represent the most effective defense against both mechanical failures and hostile security threats.

The integrated safety and security framework (IS2F)

To address the demands of operating within complex national security environments, this study proposes the Integrated Safety and Security Framework (IS2F). Building upon foundational FAA SMS and ICAO doctrines, the IS2F is specifically designed to transition the pilot-in-command from a system manager to an active tactical defender. The framework operates on four interconnected pillars:

a) Awareness (continuous threat monitoring): Beyond standard weather and NOTAM reviews, this pillar requires flight crews to maintain real-time tactical awareness of the geopolitical environment. Pilots must actively monitor for localized GPS degradation warnings, active cyber-threat advisories, and sudden shifts in ADIZ enforcement, treating environmental intelligence as a critical flight instrument.

b) Detection (systematic anomaly identification): Early detection relies on aggressive cross-verification and pattern recognition. In practice, this means crews must not passively trust automated systems. Pilots must actively compare potentially degraded GNSS signals with raw inertial data and conventional radio navigation to identify spoofing, jamming, or cyber intrusion attempts before the flight path is compromised.

c) Prevention (layered defenses and procedural discipline): Prevention is achieved through the uncompromising execution of operational barriers. This involves enforcing strict sterile cockpit protocols during high-vulnerability phases of flight and conducting rigorous, multi-layered vetting of access points on the ground to prevent unlawful interference or unauthorized flight deck access.

d) Response (structured tactical action): When a threat is detected, reaction time is critical. This pillar dictates the immediate and structured execution of contingency protocols. This includes securely communicating anomalies to ATC or military controllers, squawking appropriate emergency codes, and executing pre-planned evasive or diversionary maneuvers with precision to maintain aircraft control and comply with NORAD interception protocols.

[5]Transportation Security Administration. General Aviation Security Guidelines, TSA, 2022.

[6] EUROCONTROL. GNSS Interference and Aviation Safety Report, 2022; MITRE Corporation. Cybersecurity and Resilience in Aviation Systems, 2021.

[7] National Aeronautics and Space Administration (NASA). Aviation Safety Reporting System (ASRS) Database and Program Overview, 2021.

[8]RTCA. DO-326A – Airworthiness Security Process Specification, 2014; DO-355 – Information Security Guidance for Continuing Airworthiness, 2015.

This framework reflects a modern aviation philosophy where risk is actively neutralized through tactical foresight rather than passively avoided.

Discussion and conclusion

The seamless integration of regulatory, operational, and technical disciplines demonstrates that flight safety in the modern era is intrinsically linked to homeland defense. Safeguarding business aviation requires a trifecta of traditional operational discipline, technological resilience against emerging cyber and electronic threats, and a strategic awareness aligned with U.S. national security priorities.

This expanded perspective fundamentally elevates the role of the pilot into that of an active risk manager and defender of critical infrastructure. While U.S. business aviation is fully capable of maintaining exceptional safety standards during periods of geopolitical conflict, doing so requires a profound evolution in operational mindset.

The findings of this study establish that safety and security can no longer exist in silos; they must be treated as a unified, uncompromising system. By adopting the proposed IS2F model, the aviation industry can institutionalize early anomaly detection, technological redundancy, and disciplined response mechanisms. Ultimately, implementing this framework provides a highly scalable, practical model that directly protects U.S. airspace, ensuring that business aviation remains a secure, resilient, and vital component of the national economy and defense infrastructure.[1–11]

Acknowledgements

None.

Conflicts of interest

The author declares that there are no conflicts of interest.

Funding

None.

References

1. Federal Aviation Administration. *Advisory Circular AC 120-92D: Safety Management Systems for Aviation Service Providers*. 2024.
2. Federal Aviation Administration. *Aeronautical Information Manual (AIM)*. 2023.
3. International Civil Aviation Organization. *Safety Management Manual (Doc 9859)*. 4th ed. 2018.
4. International Civil Aviation Organization. *Annex 17: Security*. 2020.
5. EUROCONTROL. *GNSS interference and aviation safety reports*. 2022.
6. MITRE Corporation. *Cybersecurity and resilience in aviation systems*. 2021.
7. National Aeronautics and Space Administration. *Aviation Safety Reporting System (ASRS)*. 2021.
8. Transportation Security Administration. *General Aviation Security Guidelines*. 2025.
9. RTCA. *DO-326A: Airworthiness Security Process Specification*. 2014.
10. RTCA. *DO-355: Information Security Guidance for Continuing Airworthiness*. 2020.
11. North American Aerospace Defense Command (NORAD). *Aerospace Warning and Control Mission Overview*. 2020.

Citation: Kelly GS. Safeguarding U.S. airspace: an integrated safety, security, and operational resilience framework (IS2F) for business aviation in complex threat environments. *Aeron Aero Open Access J*. 2026;10(2):65–67. DOI: 10.15406/aaoaj.2026.10.00250