SKYGRID | A Boeing Company.

Addressing the Need for Comprehensive Cybersecurity in Advanced Air Mobility and Autonomous Aviation

Existing aviation cybersecurity frameworks were not designed for the distributed, cloud-connected, and highly automated systems that define Advanced Air Mobility. As autonomous flight scales, the gap between current standards and operational reality becomes a safety-critical vulnerability, and it is one that the industry must close now.

The Problem

Aviation cybersecurity standards set by the FAA, ICAO, and EASA were built for manned aircraft with physical threat boundaries. Traditional frameworks like DO-326A are narrowly scoped to onboard systems and cannot address the interconnected, cloud-reliant architectures that AAM and autonomous operations depend on.

Three critical gaps have emerged: no standard addresses the cybersecurity requirements of one-to-many autonomous operations; no framework covers end-to-end security across distributed TSP networks; and no existing guidance accounts for cyber-physical threats like GNSS jamming and spoofing that directly threaten autonomous navigation integrity.

Network and Data Disruption

A cyberattack on a TSP's network can sever real-time situational awareness data flows, risking loss of separation, collisions, or encounters with hazardous weather.

Cloud Infrastructure Risk

AAM's dependency on cloud storage and processing exposes critical flight data to ransomware, data breaches, and denial-of-service attacks at scale.

One-To-Many Cascading Failure

A single compromised TSP can simultaneously affect multiple autonomous vehicles, amplifying the safety consequences of any single cyber event.

TSPs: A New and Underprotected Attack Surface

Third-party service providers (TSPs) like SkyGrid are the digital backbone of AAM, delivering communication, navigation, surveillance, situational awareness, and decision support for both crewed and uncrewed operations. This centrality makes TSPs high-value targets. Unlike traditional onboard systems, TSPs must simultaneously secure real-time data flows between ground operators, cloud infrastructure, and airborne assets. Current standards offer no guidance for this threat model.

The Solution: NIST Cybersecurity Framework

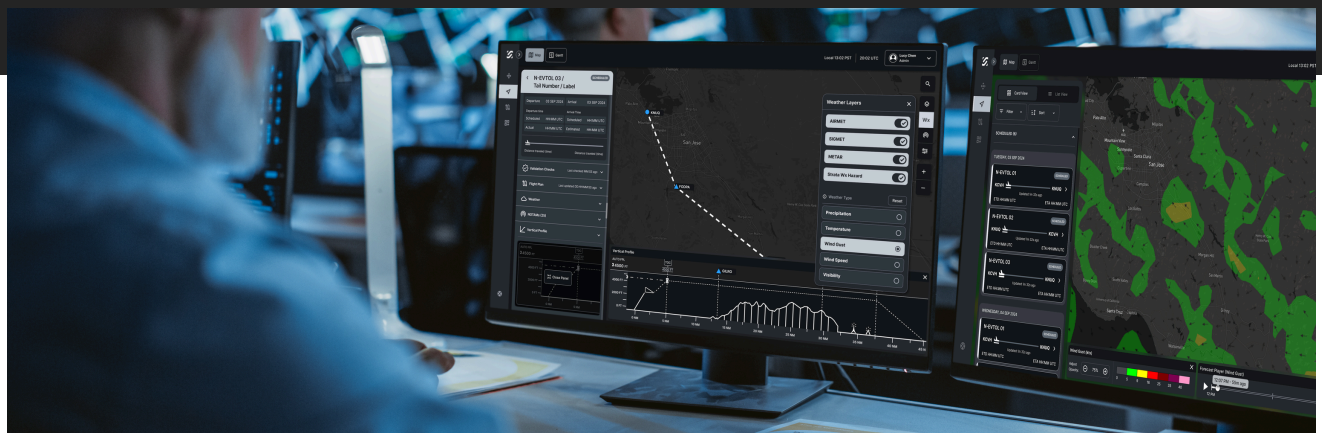
After a systematic review of EUROCAE, RTCA, and ASTM standards, SkyGrid's cybersecurity team determined that the National Institute of Standards Technology (NIST) Cybersecurity Framework (CSF) and ISO 27001 provide the most robust, adaptable model for TSP environments. Unlike DO-326A, NIST is not constrained to onboard systems; it scales across architectures, hosting environments, and threat categories.

NIST's five core functions, Identify, Protect, Detect, Respond, and Recover, support continuous monitoring and real-time threat detection essential for interconnected aviation systems. Its risk-driven approach covers both digital threats (ransomware, breaches) and cyber-physical threats (GNSS jamming, spoofing), closing the gap that aviation-specific standards cannot address.

Identify	Protect	Detect	Respond	Recover
Know your assets and risks	Safeguards and access controls	Continuous monitoring and anomaly detection	Incident response and communications	Restoration and resilience planning

Achieving TSP Cybersecurity

SkyGrid's Framework, Approach, and Industry Call to Action



SkyGrid's Cybersecurity Approach

NIST Cybersecurity Framework Aligned

SkyGrid has adopted NIST CSF as its foundational security model, applying it across both corporate governance and the PSU product platform, ensuring consistent, risk-driven protection at every layer of the stack.

ISO 27001 Information Security

An ISO 27001-aligned ISMS covers organizational policies, data handling, access controls, and incident management, providing the governance structure that underpins SkyGrid's technical cybersecurity measures.

Cyber-Physical Threat Coverage

SkyGrid's threat model explicitly includes GNSS jamming and spoofing, cyber-physical threats critical for autonomous navigation integrity that are absent from traditional aviation cybersecurity standards.

Enabling Autonomous Trust

Strong TSP cybersecurity is the precondition for autonomous aviation at scale. SkyGrid's platform enables autonomous systems to operate with reduced human oversight while maintaining full safety and regulatory compliance.

Call to Action for the Industry

The expansion of AAM and autonomous aviation demands a coordinated industry response on cybersecurity. SkyGrid's analysis makes clear that the current patchwork of aviation-specific standards leaves TSPs, and by extension, the entire AAM ecosystem, exposed. Closing this gap requires collective action from operators, regulators, manufacturers, and service providers.

SkyGrid calls on all stakeholders to actively validate the NIST Cybersecurity Framework as the foundational blueprint for AAM cybersecurity. By unifying around a proven, adaptable standard and extending it with aviation-specific guidance where needed, the industry can collectively fortify the digital infrastructure that safe, scalable autonomous aviation depends on.

Read the Full White Paper

Download "Closing the Gap: Addressing the Need for Comprehensive Cybersecurity in Advanced Air Mobility and Autonomous Aviation" at skygrid.com.

About SkyGrid

SkyGrid, a Boeing Company, exists to open the sky for autonomous flight. Based in Austin, Texas, SkyGrid builds high-assurance third-party services to enable the safe operation and integration of autonomous aircraft. SkyGrid also acts as the operational nexus for Advanced Air Mobility, integration, and managing data, infrastructure, access, and traffic to support scaled operations. For more information, visit www.skygrid.com.

SKYGRID