SMARTX
Community Exchange

# Smart Aviation: Securing Aviation Systems

*A Strategic Inititative for Digital Identity, Cyber Resilience, and Operational Intelligence in U.S. Flight Control*



www.SmartCommunityExchange.com

www.SmartCommunityPrograms.com

## Executive Summary

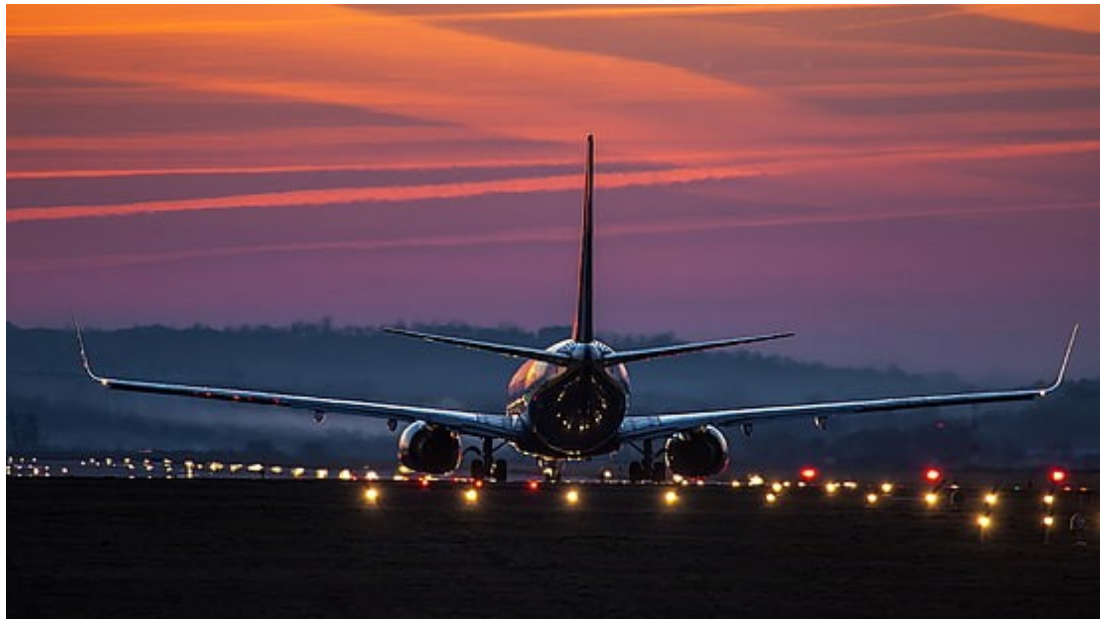
This executive summary outlines the deployment of a national security pilot utilizing **PeAN (Personal Access Node) devices**—an intelligent, secure, and AI-enabled communication platform designed for high-integrity environments. The project aims to bolster aviation resilience by enabling real-time, encrypted communication between air traffic controllers, pilots, ground crews, and secure flight systems.

The PeAN platform supports **digital identity verification**, **zero-trust cybersecurity**, and **AI-assisted anomaly detection**, making it a powerful tool to modernize and secure national flight control infrastructure in collaboration with FAA, DHS, and airport authorities.

## Background and Rationale

Amid rising threats to aviation cybersecurity and increasing autonomous operations, current flight control systems rely heavily on legacy communication protocols and fragmented credentialing. In 2023, the U.S. Government Accountability Office (GAO) highlighted the urgent need for improvements in airspace cybersecurity and ground-to-air resilience.

PeAN's encrypted node system directly responds to this need. When embedded into the personnel, assets, and infrastructure of aviation stakeholders—from local airports to national command centers—it creates a **secure, contextual, intelligent network** across U.S. air traffic operations.



## Project Goals and Objectives

**Deploy PeAN wearable and infrastructure nodes** in airports and FAA testbeds.

**Enable secure, continuous communication** between control towers, aircraft, autonomous vehicles, and emergency systems.

**Authenticate digital identities and task credentials** for flight controllers, field technicians, and federal agents.

**Detect and isolate cybersecurity anomalies** in real time through AI and behavior modeling.

**Create a national blueprint** for PeAN-powered flight control expansion through FAA, DHS, DoD, and allied partners.

## Key Use Cases

**Redundant Air-Ground Communications** in the event of radio or data line failure

**Cyber Intrusion Defense** via biometric and behavioral identity-linked device access

**Emergency Routing Protocols** supported by automated geofencing and first responder coordination

**ATC Personnel Credentialing and Role-Based Access Control** using programmable PeAN IDs

**Autonomous Aircraft Support** including electric cargo drones and UAM corridors

## Implementation Plan

**Phase 1: Design & Stakeholder Alignment** (Months 1–3)

- Partner with FAA, TSA, DHS CISA, airport CTOs
- Refine use case prototypes for secure PeAN deployment

**Phase 2: Deployment & Training** (Months 4–16)

- Device deployment to ATC, flight crews, and emergency teams at test airports
- Training modules and compliance with FAA cybersecurity and operational standards

**Phase 3: Live Pilot & Data Collection** (Months 17–20)

- Monitor performance and resilience under operational conditions
- Independent evaluation of threat detection, user experience, and communications uptime

**Phase 4: Evaluation & National Blueprint Development** (Months 21–24)

- FAA briefing and interagency recommendations for national rollout
- Integration plan with NextGen and airport resilience frameworks

## Outcomes and Impact

- Increased ATC response accuracy and reduced miscommunication risks
- Nationally replicable model for aviation cybersecurity modernization
- Stronger coordination between federal, state, and airport-level aviation security
- Creation of a secure digital infrastructure to support U.S. air mobility innovation
- Scalable system for domestic use and allied international adoption (e.g., NATO partners)

SMARTX Community Exchange

**Strategic Partners and Supporters**

Enterprises and organizations, federal and aviation security, academic R&D, CISA, TSA, Innovation Task Force, Airports, Carriers, Regional Innovation and Tech Hubs, CTO Alliance

## Next Steps

We welcome the opportunity to present this proposal and begin collaborative design of the project framework.

A comprehensive executive presentation, technical blueprint, and partner MOU drafts can be prepared upon request.