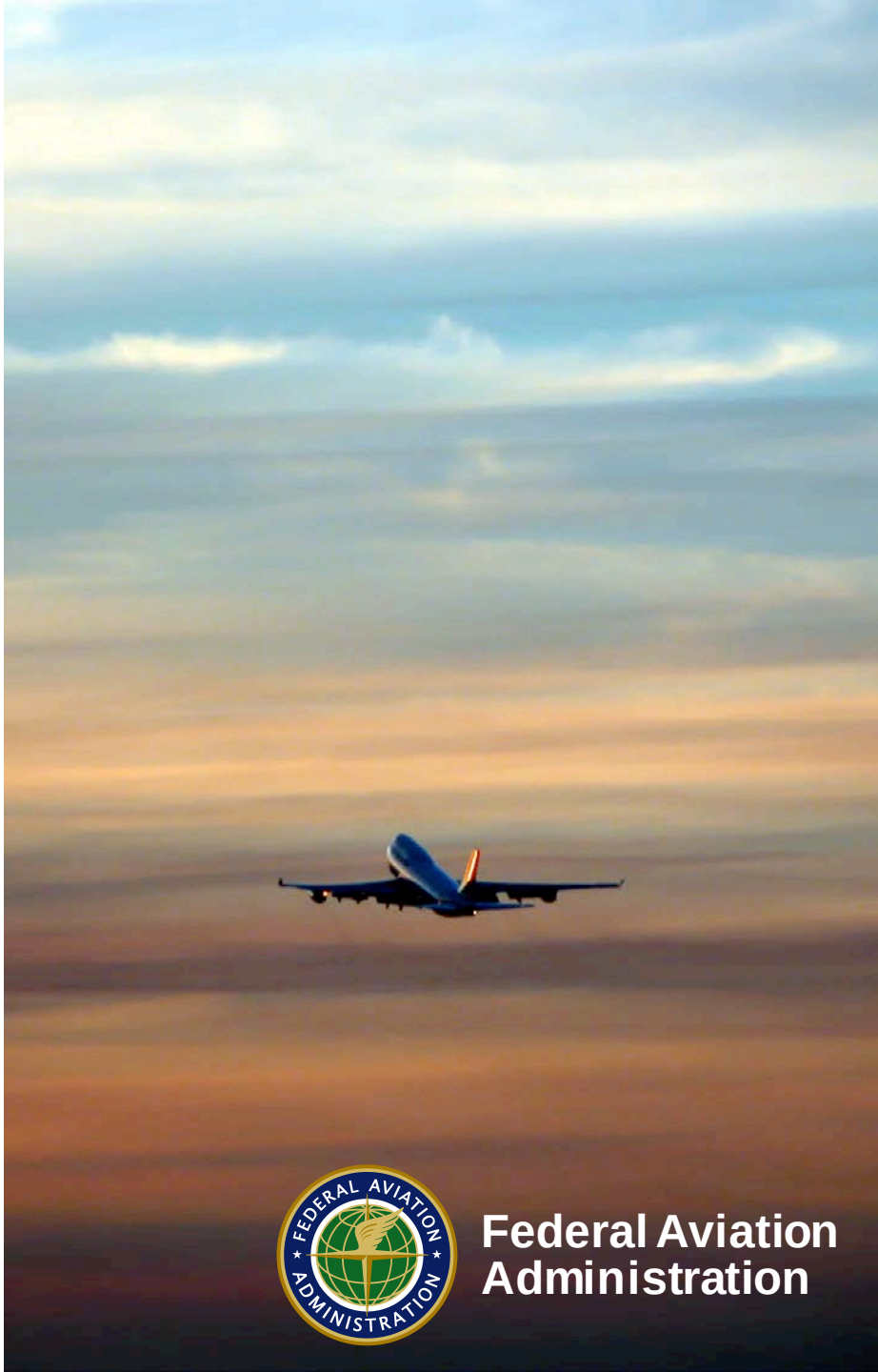
Airport Cybersecurity Risk

The Federal Government Perspective

Presented to: ACI-NA BIT Committee

By: Philip Windust, Aviation Ecosystem Stakeholder Engagement (AIS-030)

Date: September 14, 2019



Airport Cybersecurity: Overview

- **Over 19,000 airports nationwide**
  - 520+ that hold an FAA Operating Certificate under Part 139
  - Approximately 450 that hold a TSA Security Program
  - 385 primary airports (>10,000 annual passenger enplanements)
- **Each airport is a unique association of Federal, State, and local governmental entities, companies and organizations**
  - Diverse IT and OT systems
  - Inconsistent standardization
  - Varying risk perspectives
- **Challenging effort to secure multiple systems operated by multiple owners**

Airport Cybersecurity: Issues and Challenges

- **Cyber risk in the airport environment is evolving**
  - Adversaries are improving and adapting their capabilities
  - Additional technologies are expanding the attack surface
  - Even isolated accidental outages have had significant financial impact; intentional and malicious attacks could erode public trust and confidence
- **Effectively mitigating this evolving risk will require collaboration among all stakeholders**
  - Improve information sharing between governmental and private sector stakeholders
  - Develop a shared understanding of threats, vulnerabilities, and potential consequences
  - Generating shared responsibility for reducing risk

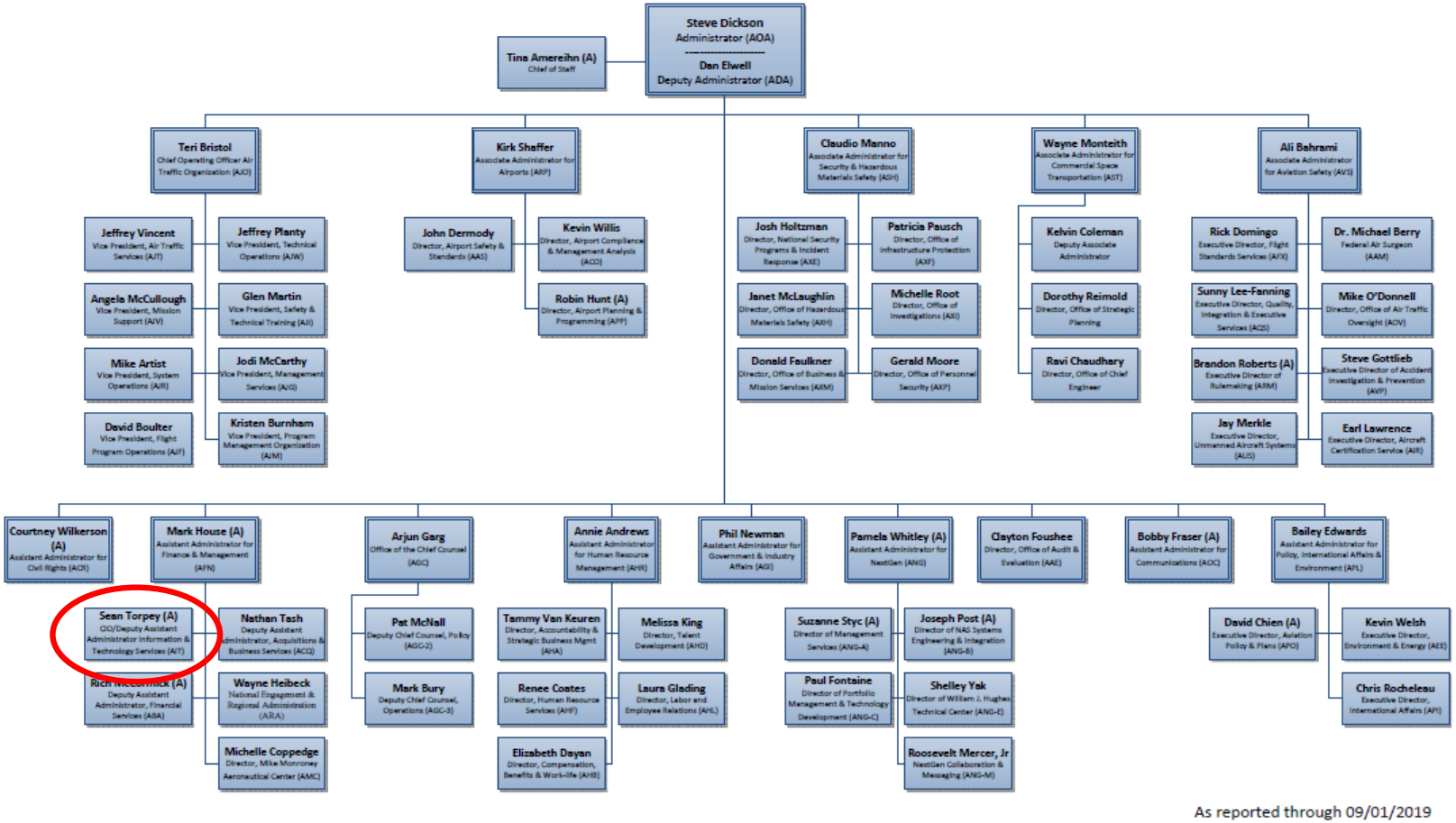
What is the Federal Government Doing?

- **Federal Aviation Administration (FAA)**
  - Established the Aviation Ecosystem Stakeholder Engagement Office
  - Evolving Cyber Safety Commercial Aviation Team (Cyber Safety CAT)
- **Transportation Security Administration (TSA)**
  - Published the Cybersecurity Roadmap
  - Developing cyber incident sharing guidance
- **Aviation Cyber Initiative (ACI)**
  - Charter developed and signed in May 2019
  - Suite of training and services available to the airport community

Federal Aviation Administration (FAA)

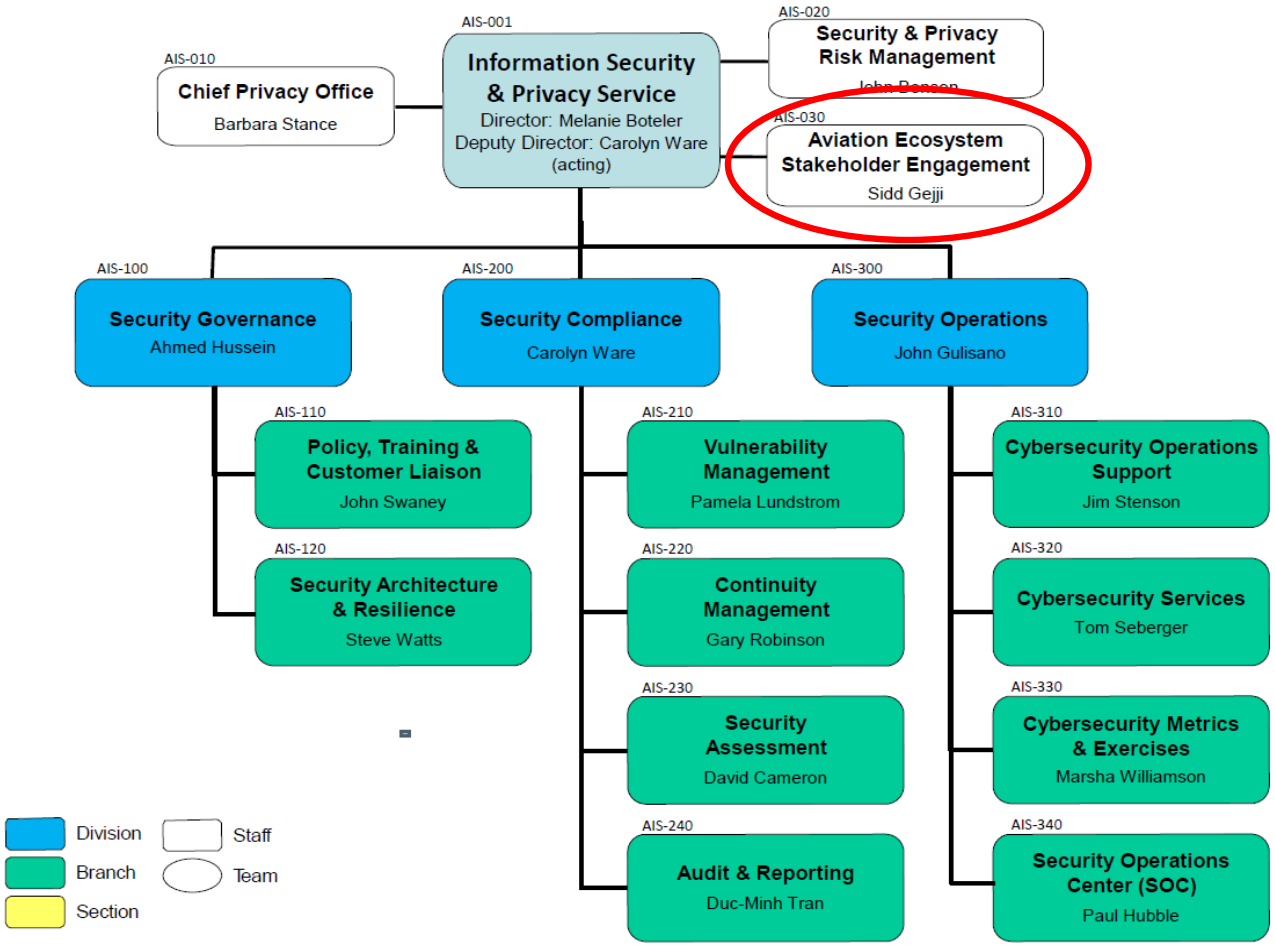
- **Aviation Ecosystem Stakeholder Engagement Office**
  - MISSION: Understand aviation ecosystem cybersecurity risk and collaborate with stakeholders to enable improved resiliency
  - Established in 2018, reporting to the CISO
  - Specialists focusing on 4 major elements of the ecosystem: airports, airlines, aircraft, and air traffic management
  - Close collaboration with FAA Office of Airports
- **Cyber Safety Commercial Aviation Team (Cyber Safety CAT)**
  - Safety Risk Assessment (SRA) Methodology and Risk Based Decision Making (RBDM) Process established
  - Originally developed to address aircraft cybersecurity risk, but potential adoption by all elements of the aviation ecosystem

Aviation Ecosystem Stakeholder Engagement



As reported through 09/01/2019

Aviation Ecosystem Stakeholder Engagement



Transportation Security Administration (TSA)

- **Published the TSA Cybersecurity Roadmap**
  - Articulates TSA's cybersecurity strategy is support of the National Cyber Strategy and DHS Cybersecurity Strategy
  - Several goals related to the Transportation Systems Sector (TSS) that seek to understand cybersecurity risk posture and support risk management activities
- **Developing cyber incident sharing guidance**
  - Intent is to better understand the threat environment in order to more effectively assess cybersecurity risk

Aviation Cyber Initiative (ACI)

- **Tri-Chaired Task Force led by chairs from the Departments of Homeland Security (DHS), Transportation (DOT), and Defense (DOD)**
  - Charter signed in May 2019 by the Secretaries of DHS, DOD, and DOT
  - Will implement the cybersecurity objectives of the National Strategy for Aviation Security (NSAS)
- **Mission**
  - Reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem

Aviation Cyber Initiative (ACI)

- **Working Groups**
  - Execute the ACI Charter, Mission, and Supporting Objectives
  - 10 existing or planned WGs, including Airports
  - Airports WG will seek to identify and monitor small, medium, and large airport cyber risk reduction and resilience initiatives, identify best practices and improvement opportunities, and establish a persistent engagement program with airport CISOs
- **Training and Services**
  - Aviation Ecosystem Assessment / Validated Architecture Design Review (VADR)
  - Airport WiFi Assessment Cybersecurity Training
  - ICS Cybersecurity 301

Aviation Ecosystem Stakeholder Engagement

Philip Windust

Aviation Ecosystem Stakeholder Engagement Office
Office of the Chief Information Security Officer
Federal Aviation Administration
philip.b.windust@faa.gov
202.267.8754 (office)
703.589.0920 (mobile)

Aviation Ecosystem Stakeholder Engagement Office Shared Account:
AviationEcosystem@faa.gov