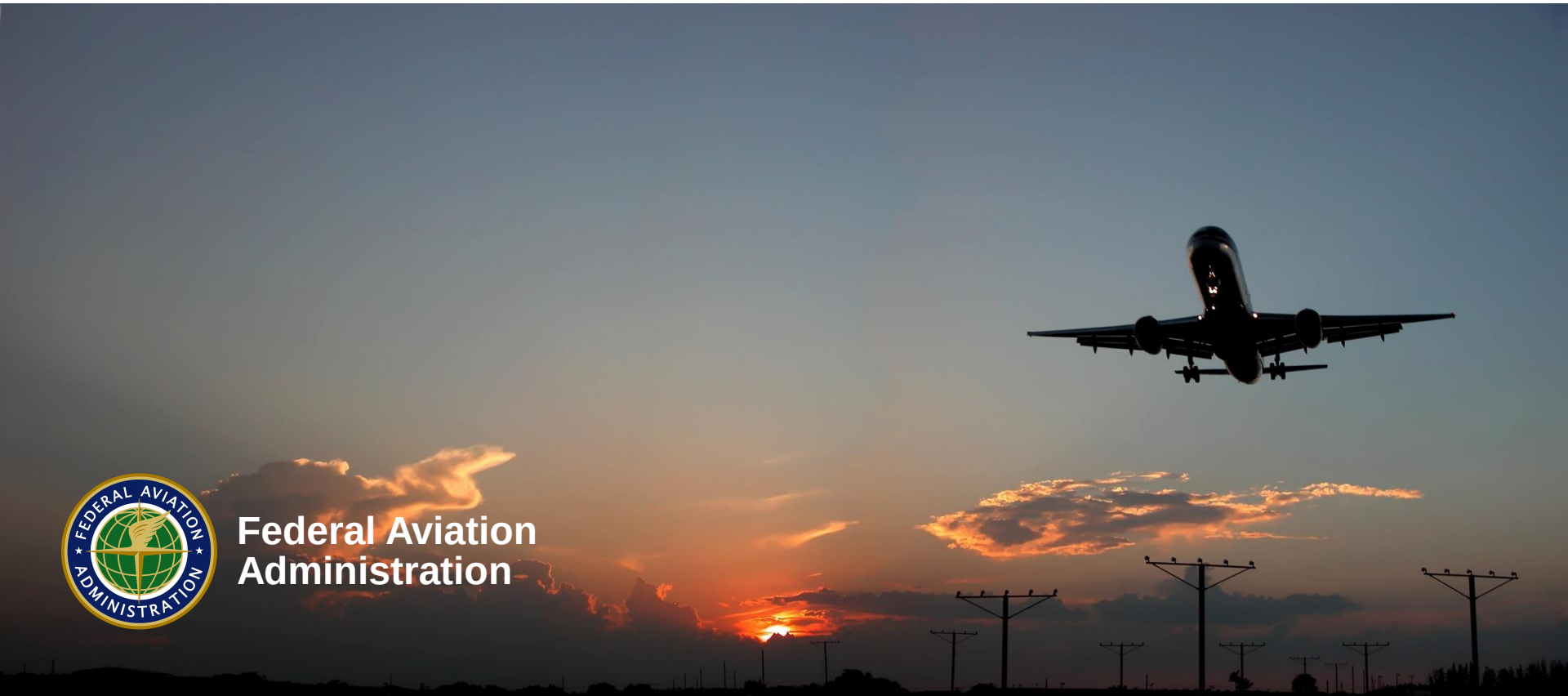
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

Program Control & Governance (PC&G)

Date: October 20, 2020



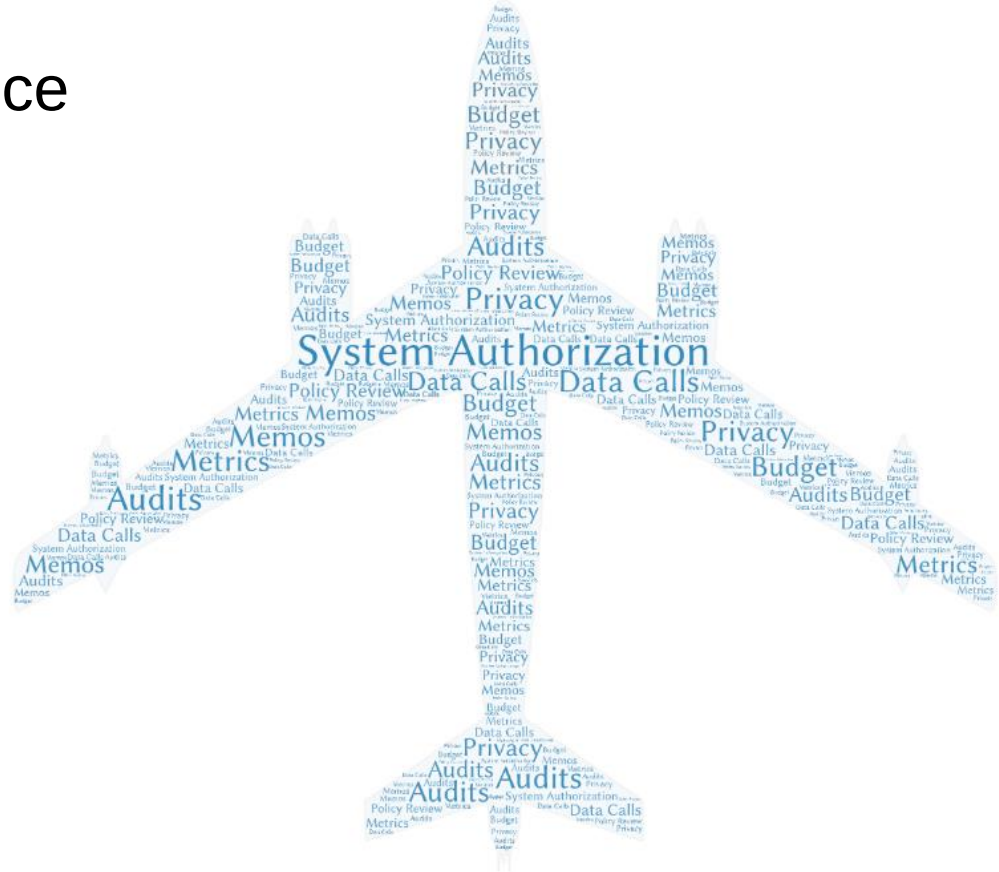
Mission

To provide oversight across the Air Traffic Organization (ATO) Cybersecurity Group and to guide, manage, and track the lifecycle of ATO National Airspace System (NAS) and Mission Support systems through the Information Security Continuous Monitoring (ISCM) Authorization process.

PC&G

Primary Functions

- Information Assurance (Authorization)
- Privacy
- Audits
- Data Calls
- Policy
- Memos
- Metrics
- Budget



Information Assurance (Authorization)

PC&G manages the Authorization Process, including:

- Managing and tracking the Master Authorization and Information Security Continuous Monitoring (ISCM) Schedule
- Authorization document finalization
- Coordination of security testing
- Information System Security Officer (ISSO) system and domain assignments
- Authorization package signature process
- Reporting and Statistics

Privacy

PC&G manages the Privacy processes within the Air Traffic Organization (ATO), including development and tracking of:

- Privacy Threshold Analyses (PTAs)
- Privacy Impact Assessments (PIAs)
- Privacy Continuous Monitoring Documents
- ATO Privacy Training

Why? Privacy Act of 1974, eGov Act, Office of Management & Budget (OMB) Memorandums

- Legal requirement to protect & inform citizens on how their data is used

Audits

PC&G coordinates and consolidates responses to audits from various internal and external organizations:

- Federal Aviation Administration (FAA) Office of Information Security & Privacy (AIS)
- Department of Transportation (DOT) Office of the Inspector General (OIG)
- General Accountability Office (GAO)
- Department of Homeland Security (DHS)

Data Calls

PC&G manages and coordinates responses to data calls

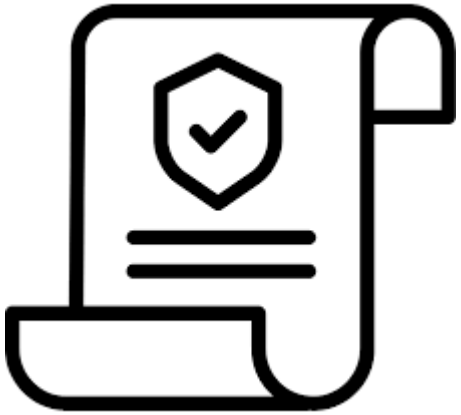
Most data calls involve urgent security issues and may originate from:

- FAA Security Operations Center (SOC)
- National Airspace System (NAS) Cyber Operations (NCO)
- DHS:
  - Binding Operational Directives (BODs)
  - Emergency Directives (EDs)

Policy Development and Review

Purpose:

- To ensure cybersecurity is appropriately and accurately addressed in the document.
- To ensure the document content adheres to (does not contradict) ATO Cybersecurity Group, ATO, FAA, and DOT orders and ATO/NAS requirements.

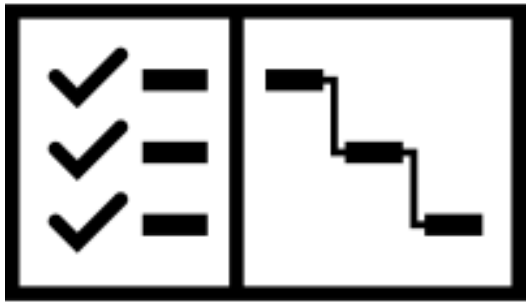


Function:

- Reviews are performed in conjunction with all ATO Cybersecurity Group teams.
- Documents include:
  - Draft Orders (FAA, DOT)
  - Notices
  - Guidance Documents

Program Management

PC&G tracks the following for the ATO Cybersecurity Group:



- Standard Operating Procedures
- Program Management Plans
- Memos
- Funding Allocation and Expenditure

Metrics

PC&G tracks and reports metrics for:

- **Authorization**
  - Number of systems authorized for fiscal year
  - Authorization documents completed

- **Electronic signatures (time in queue):**
  - Authorization packages
  - Memos
- **Plan Of Action & Milestones (POAMs):**
  - Number and percent finalized and completed
  - Criticals, Highs, Mediums, and Lows
  - By Organization and by System

Budget

Primary Budget Areas:

- **Operations (Ops)**: Funds the administration, operation, repair, and maintenance of the NAS
- **Facilities & Equipment (F&E)**: Provides for current infrastructure, modernization, and the advancement of NextGen Air Traffic Control
- **Capital Planning and Investment Control (CPIC)**: A systematic approach to selecting, managing, and evaluating information technology investment
  - ATO Cybersecurity Group submits and collects security costs on behalf of ATO NAS systems
- **Enterprise Remediation**: The ATO Cybersecurity provides funding to systems to close out POAMS as prioritized by the Deputy Vice Presidents.