

2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem / “Cyber Hygiene”

Information Security & Privacy Service

Date: October 20, 2020



Federal Aviation
Administration



Security Governance

- **Security Governance Division serves as the authority for ensuring effective governance throughout IS&P.**
 - They specify the accountability framework, ensure that security strategies are aligned with business objectives, adhere to policies and internal controls, and are consistent with applicable laws and regulations.
 - This division closely works with each LOB/SO relation to:
 - Identification of Key ISS Personnel (significant security responsibilities).
 - Completion of annual Specialized Role-Based Training requirements.
 - Development of the policies, management, visibility, and processes information system lifecycle management support.
- **Functional Areas:**
 - Policy, Training & Customer Liaison Branch
 - Security Architecture & Resilience Branch



Functional Area of Responsibility

Policy, Training & Customer Liaison Branch

- **Develop and update FAA policies to ensure security and privacy requirements are addressed, interpret policy and other regulatory requirements related to cybersecurity, and assist with developing standard operating procedures (SOPs) and policy positions for the agency.**
 - They oversee the FAA's annual Security Awareness Training (SAT), and other information security and privacy training as needed.
 - They serve as customer liaisons (ISSM/ISSO/Privacy Managers) to the agency's Lines of Business and Staff Offices and facilitate services, information flow, and remediation activities.
 - In addition, they process cybersecurity, information security and privacy deviations and waivers not included in System Authorizations.
 - Include services we provide, our process, timelines.

Functional Area of Responsibility

Security Architecture & Resilience Branch

- **Members of this branch work with other Security Divisions, Staff Offices and agency POCs to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.**
 - They develop and maintain AIT's Continuity of Operations (COOP) plan and they support and ensure maintenance of the FAA's Security Architecture.
 - They develop, coordinate and maintain the Reconstitution for FAA HQ (AWA) plan.
 - They develop and maintain the Mission Support cybersecurity architecture repository and data models consistent with the Enterprise Cybersecurity Architecture to enable sharing across FAA domains.