2020
FAA CYBERSECURITY AWARENESS SYMPOSIUM
THEME – "CYBER HYGIENE"

INFORMATION SECURITY & PRIVACY SERVICE (AIS)

The Information Security & Privacy Service (IS&P) fortifies the security of the FAA's network and infrastructure, including the three domains:

- Mission Support
- NAS
- Research & Development (R&D)

To safeguard the agency and its personnel, IS&P manages accountabilities in the three domains, develops IT security policies, ensures compliance with FAA security policies and security/privacy controls, maintains Continuity of Operations (COOP) plans, supports the FAA's Architecture, provides tooling resources, supports cyber exercises, and through the SOC, provides 24x7 monitoring and technical support to detect security threats and attacks against the agency.

Major Functions:

- Performs the role of the Chief Information Security Officer (CISO).
- Responsible for developing, issuing, updating, and carrying out the FAA Enterprise Information Systems Security and Privacy Program.
- Advises the Risk Executive of risk acceptance disagreements between the CISO and Authorizing Official.
- Provides expertise and oversight for privacy requirements across the FAA.
- Provides guidance for the protection of Personally Identifiable Information (PII) and privacy records.
- Manages the Identity Monitoring Code issuance process, responds to FAA privacy incidents, and oversees the handling of privacy requests, appeals, and complaints.

Major Functions (cont.):

- Implements accountability and continuous improvement of FAA privacy processes and programs, reviews and approves privacy compliance documentation, including Privacy Threshold Analysis (PTAs), Privacy Impact Analysis (PIA), and privacy assessments, and provides updates to System of Record Notices (SORNs).
- Provides enterprise Security Risk Management support, and leads the assessment, determination, and correlation of quantitative and qualitative values of security risk related to an identified situation and a recognized threat.
- Develops and updates FAA IT Security policies to ensure security and privacy requirements are addressed, interprets policy and other regulatory requirements related to cybersecurity, and assists with developing standard operating procedures and policy positions for the agency.
- Oversees the FAA's annual Security and Privacy Awareness Training, Information Security System (ISS) cybersecurity personnel role based training, and other information security and privacy training as needed.
- Serves as customer liaisons to the Agency's LOBs and SOs and facilitate services, information flow, and remediation activities.
- Establishes and supports the AIT Intake processes for IS&P established by BPS which serves as the front door into IT services.
- Develops and maintains AIT's COOP plans, supports and ensures development of the FAA's Security Architecture.

2020
FAA CYBERSECURITY AWARENESS SYMPOSIUM
THEME – "CYBER HYGIENE"

INFORMATION SECURITY & PRIVACY SERVICE (AIS)

Major Functions (cont.):

- Responsible for assessing information system compliance with federal, DOT, and FAA policies, standards, and controls.
- Monitors/tracks security vulnerabilities, coordinates vulnerability scans, monitors/tracks security incidents, DR exercises, Information System Contingency Plan (ISCP) and ISCP testing to include Business Impact Assessments.
- Responsible for Audit and Reporting on data calls from Office of Inspector General and General Accounting (GAO), Federal Information Security Management (FISMA), Capital Assessment Project goals, Section M contract reviews and privacy compliance act reviews.
- Provides services related to monitoring and tracking vulnerabilities within the FAA's FISMA reportable systems.
- Ensures Plan of Action & Milestones (POA&Ms) are entered into the Cyber Security Assessment and Management (CSAM) system.
- Monitors and tracks the POA&Ms, provides support to stakeholders on remediation/mitigations, the quarterly review of open POA&M's with System Owners and processes and coordinates MOAs/Memorandum of Understanding (MOUs), coordinates vulnerability scanning, monitors/tracks security incidents, monitoring and tracking binding operational directives and responds to audits related to POA&Ms.

Major Functions (cont.):

- Manages vulnerability mitigation and remediation as identified by the FAA's Data Loss Prevention (DLP) service security assessments, vulnerability scans and incident events.
- Manages vulnerability mitigation and remediation of all Department of Homeland Security (DHS) Cyber Hygiene scanning vulnerabilities.
- Responsible for scheduling, conducting, and tracking security assessments.
- Maintains the Agency's FISMA-reportable IT inventory and required system data in the DOT FISMA Reporting System of Record, CSAM.
- Provides audit and data call Agency liaison coordination services for a variety of audits, including Financial Statement audits, FISMA audits, Office of Inspector General audits, Government Accountability Office audits, and the Cybersecurity Act of 2015 also known as Cybersecurity Information Sharing Act.
- Provides the services needed to detect, analyze, respond to, report on, and ultimately prevent cybersecurity incidents.
- Provides incident response, advanced persistent threat analysis, intrusion detection, and forensic analysis services for the FAA Enterprise.
- Consolidates cybersecurity functions by performing the day-to-day activities needed to mitigate IS&P risks at the technical level.
- Hosts the FAA's SOC which provides 24x7 monitoring and technical support to detect security threats and attacks against the FAA.