**U.S. DEPARTMENT OF TRANSPORTATION**
FEDERAL AVIATION ADMINISTRATION
Information and Technology National Policy

**ORDER**
**IT 1100.171A**

Effective Date:
08/01/2020

**SUBJ:** Office of Information and Technology (AIT) Organization

This order describes and provides the Office of Information and Technology's (AIT) mission, functions, responsibilities and organizational structure to the lowest level. The organizational structure, including functions at the director level, is documented in the current edition of Federal Aviation Administration (FAA) Order 1100.1, FAA Organization—Policies and Standards.

The FAA Chief Information Officer (CIO) is the principal adviser to the Administrator and to the Lines of Business (LOBs) and Staff Offices (SOs) on matters involving Information Technology (IT) management, and has primary FAA oversight responsibility for all Agency IT investments. The CIO promotes and guides FAA IT direction and implementation that foster agency goals for improving "safety, mobility, global connectivity, environmental stewardship, security, and organizational excellence. To monitor FAA IT activities and measure progress, the CIO organizational components and work activities include the following:

- Immediate Office of the Chief Information Officer/Information & Technology (AIT-1)
- Strategy & Performance Service (ASP-1)
- Enterprise Program Management Service (AEM-1)
- Business Partnership Service (APS-1)
- Solution Delivery Service (ADE-1)
- Infrastructure & Operations Service (AIF-001)
- Information Security and Privacy Service (AIS-001)
- Chief Data Office (ADO-1)

Revisions to this order should be made based on the organizational needs, and management's consideration and approval. AIT's Policy and Administrative Branch (ASP-110) is responsible for the maintenance of this order.

KRISTEN K. BALDWIN
Digitally signed by KRISTEN K. BALDWIN
Date: 2020.07.28 18:03:10 -04'00'

Kristen Baldwin
Deputy Assistant Administrator
for Information & Technology and CIO, AIT-1

# Chapter 1. General Information

**1. Purpose of this Order.** This order describes the organizational structure, mission, functions, and responsibilities of the AIT in the Office of Finance and Management (AFN).

**2. Audience.** This order affects all organizations and external parties who receive services from AIT and interface with FAA IT and infrastructure systems.

**3. Where Can I Find This Order?** This order is available on the MyFAA employee website; https://employees.faa.gov/tools_resources/orders_notices/ and on the public website; https://www.faa.gov/publications_polices/orders_notices/.

**4. Reference.** Department of Transportation (DOT) Order 1351.39 IT Governance Policy; CIP Chapter 1351.39; Departmental Information Technology Governance Policy.

**5. Federal Information Technology Shared Services Strategy.** In 2010, the Office of Management and Budget (OMB) released the *Federal IT Shared Services Strategy*, which further emphasizes the need for agencies to use a "Shared-First" approach to IT service delivery. The overall plan is to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions.

## Chapter 2. Information & Technology (AIT)

**1. Deputy Assistant Administrator for Information & Technology/Chief Information Officer (AIT-1/CIO).**

a. Has authority to make changes in AIT structure, and authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below.

b. This office provides leadership and management for secure enterprise-wide information technology services to support the FAA's mission. The AIT organization is managed by AIT-1/CIO and Deputy Director AIT/Deputy CIO, AIT-2, and is comprised of seven (7) service offices.

c. AIT-1 is the FAA's CIO principal IT, cybersecurity, privacy, and records management advisor to the Administrator, and is the final authority on these matters within the Agency. The Office of the CIO supports the FAA Strategic Goals of Safety, Innovation, Accountability and Infrastructure by providing leadership on all matters associated with the Agency's IT portfolio. The CIO participates with each IT Service Director in the strategic direction and oversight of agency initiatives under their scope and authority.

d. FAA's Deputy CIO (AIT-2) is the senior advisor to the FAA CIO for all matters including policy, budget formulation, planning, execution, and oversight. The Deputy CIO is responsible for effectively leading AIT on a day-to-day basis, overseeing the budget and the activities of employees engaged in IT management and service delivery.

e. FAA's office of the CIO/Deputy CIO (AIT-1/2) is responsible for the approval of all agency wide external hiring actions for positions in the technical series 2210 (Information Technology Management Series). This pertains to the hiring of new FAA employees into the 2210 series. The CIO/Deputy is also responsible for obtaining approval from the DOT CIO for said positions.

f. FAA's office of the CIO/Deputy CIO (AIT-1/2) is responsible for the approval of all agency wide IT procurement actions that are in accordance with the FAA Acquisition Management System (AMS). This pertains to AMS Policy 3.8.2.5 and AMS Guidance T3.2.1.

g. Serves as the Chairperson, IT Shared Services Committee (ITSSC). The purpose of the ITSSC is to direct the effective, secure, and cost-efficient application of Mission Support information technologies, related personnel resources and funding to meet the FAA's business needs, consistent with the goals of the FAA's IT Shared Services Transformation Plan and the FAA IT Shared Services Strategy.

h. The CIO follows guidelines as outlined in DOT Order 1351.39 IT Governance Policy, Section 39.5.

**2. Mission.** AIT's mission is to deliver core IT services to keep FAA's employees connected and productive. AIT drives transformative IT efforts that move the FAA enterprise forward; and as a trusted advisor to our business partners, develops innovative IT solutions to solve complex challenges.

**3. Temporary Special Program Office.** Each office director is authorized to have Temporary Special Program offices in support of their missions and provides input on FAA policies and procedures for which the directorate has oversight. The functional elements of these Temporary Special Program offices are under the direction of the office Director.

**4. Line of Succession.** In the event that AIT-1 is unable to fulfill their duties, the following line of succession will apply:

a. Deputy CIO, Information & Technology (AIT-002);

b. Director, Information Security and Privacy Service (AIS-001); or

c. Director, Infrastructure & Operations Service (AIF-001).

**5. Authority to Change this Order.** AIT-1/CIO is authorized to make changes as appropriate to this order through the directives management process.

# Chapter 3. Strategy & Performance Service (ASP)

**1. Director of Strategy & Performance Service (ASP-1).**

**a. Roles and responsibilities:**

(1) Has authority to make changes in ASP structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA IT policy and procedures as directed by the CIO;

(2) Provides day-to-day management of the AIT organization's foundational support activities;

(3) Delivers vendor and acquisition management support to FAA IT;

(4) Provides management and oversight of the IT portfolio and investments;

(5) Provides centralized management of FAA software licenses inventory and currency;

(6) Defines and measures enterprise effectiveness against the IT strategy;

(7) Develops policy, maintains reference documents and ensures compliance;

(8) Leads the FAA IT strategic planning process;

(9) Provides management and oversight of strategic initiatives to ensure organizational alignment;

(10) Supports staffing and resource management, leads workforce development initiatives; coordinates AIT employee training; and

(11) Provides organizational IT Contracting Office Representative (COR) services.

**b. Mission:** ASP provides the AIT organization optimal business solutions in strategic alignment with Agency goals and objectives. ASP is responsible for IT policies, processes, investment portfolio, and Talent Resources. In alignment with OMB/Agency mandates S&P provides Hardware and Software Asset Management, Software Compliance, Lifecycle Management, and IT Acquisition Strategy and Support.

**c. Vision:** ASP provides innovative, strategically relevant, and integrated business services that improve FAA IT performance, enabling our customers to focus on the execution of their mission.

**2. Workforce Development Staff Office (WDSO) (ASP-003).** Works to align employee and manager resources with AIT strategies, creating a "Future Ready" workforce by focusing on continuous development of knowledge, skills, and abilities linked to AIT's strategic plan. The staff serves as a conduit to expedite employee actions through coordination between AIT, AFN, and Office of Human Resource Management (AHR). The staff works across organizational boundaries to formulate and develop near-term and long-range workforce planning strategies for

AIT to optimize resources, identify and fill workforce gaps. Ensures learning and development supports AIT strategies and develops initiatives to support ongoing employee development and engagement opportunities. WDSO provides guidance and support to AIT leaders across all AIT service organizations to establish and maintain the foundational roadmap for the FAA IT workforce of the future.

**a. Resource Management:**

(1) Expedites employee actions through the coordination between AIT, AFN and AHR;

(2) Provides guidance and support to AIT leaders across all AIT service organizations; and

(3) Works within the AIT Resource Management team to perform organizational and personnel management functions such as personnel actions, re-organizations, performance management, hiring, policy, and document management.

**b. Training and Education:**

(1) Aligns employee and manager learning and development with AIT strategies;

(2) Researches and provides training opportunities for AIT Managers and employees to assist in leadership and employee development, to include best pricing, low/no cost opportunities to provide cost savings and efficiencies;

(3) Works within the Electronic Learning Management System (eLMS) to assist in providing managers and employees with eLMS system functionality, update training records, and provide reporting to leadership;

(4) Assists in providing managers and employees with eLMS system functionality to allow for self-sufficiency in searching and retrieving training information; and

(5) Processes training request forms and subsequent acquisition requests for AIT managers and employees.

**c. Workforce Development Initiative:**

(1) Works across organizational boundaries with AIT leaders to formulate and develop Strategic and Operational workforce plans for AIT to create a “Future Ready” workforce focused on resource alignment and continuous development of knowledge, skills, and abilities linked to AIT’s strategic plan; and

(2) Establishes and maintains the programs and processes for AIT designed to improve employee engagement, increase career development opportunities and further align learning and development strategies.

**3. IT Strategy, Policy & Business Planning Division (ASP-100).** This division provides support services for the business of IT. ASP-100 concentrates on IT strategy, policy, and business management.

**a. Policy & Administration Branch (ASP-110):**

(1) Coordinates and maintains IT-related policies, and provides program management and oversight for the FAA Directives, Forms, Orders, National Archives and Records Administration, Records Management, Paperwork Reduction Act, and Section 508 Compliance;

(2) Manages and supports the AIT Business Management System; and

(3) Serves as the point of contact (POC) for matters related to FAA administrative systems, employees and space.

**b. IT Strategy & Investment Portfolio Branch (ASP-120):**

(1) Assesses the effectiveness of the investment process and refines investment-related policies and procedures. Evaluates the IT investment portfolio to assess business value and makes recommendations to optimize investments;

(2) Builds a structured approach to categorize, evaluate, prioritize, and manage IT investments;

(3) Supports the development, execution, and tracking of spend plans for AIT, and tracks IT spending allocations across projects and departments to enhance fiscal stability;

(4) Works with teams across AIT to document processes and procedures, and provides AIT performance dashboards; and

(5) Collects and maintains data required for budget and Business Plan analysis reports.

**4. IT Enterprise Software Management Division (ASP-200).** Provides Enterprise Vendor Management and Software Asset Management for all of the FAA. This division provides Software COR support for the day-to-day software contract strategy and metrics. ASP-200 provides FAA Strategies Sourcing for the Acquisition of Various Equipment and Supplies (SAVES) contract.

**a. Vendor Management & Strategy Branch (ASP-210):**

(1) Manages the FAA’s enterprise software licensing and maintenance agreements, and serves as the vendor lead/COR for software licensing requirements;

(2) Manages the FAA’s number of user count for each agreement and oversees software licensing and maintenance currency for the FAA workforce;

(3) Works with contracting office and vendors to negotiate the best pricing position for the FAA on software acquisitions;

(4) Conducts internal reviews of installed software products to ensure compliance with FAA agreement, and collaborates with vendors to make adjustment/true-ups to maintain license currency;

(5) Serves as the FAA's central POC for software management, reporting, and exchange of information with DOT and other Federal agencies to comply with the Federal Information Technology Acquisition Reform Act (FITARA) and other OMB reporting on FAA Software acquisitions and ownership;

(6) Serves as the FAA's central POC for performing and maintaining a software inventory baseline and implementing a software harvesting process;

(7) Facilitates the National Software board to review software requests for compatibility in the AIT environment; and

(8) Concentrates on Life Cycle Governance over Software as a Service utilization.

**b. Category & Quality Branch (ASP-220):**

(1) Is responsible for the development of a risk management framework to understand current and future risks of software procurement as they relate to vendor prioritization and engagement. It is responsible for establishing category management policy memoranda and new policies for the inventory management of Commercial off-the-shelf software license;

(2) Assists in AIT Strategic Planning Identifies IT initiatives from other LOB business plans and strategies. Analyze and determine correlations between the AIT strategy and AIT portfolio of services descriptions then presents these findings to the Information Management Team. Assists the AIT Enterprise Architecture team with the development of a management roadmap for AIT strategic capabilities;

(3) Explores, evaluates and conducts proactive strategic research and analysis of emerging and innovative technologies. Provide a single point of entry for potential technology partners in order to maximize innovation opportunities and to reduce the number of industry calls and emails across AIT;

(4) Provides CIO coordination and processing. Coordinates with FAA organizations on requests for FAA acquisitions over $250K subject to review and approval by the FAA CIO or delegate in accordance with the FAA AMS.

**5. IT Asset & Purchase Management Division (ASP-300).** ASP-300 oversees all FAA IT assets that are procured, managed, or otherwise determined by FAA management or policy to be the responsibility of IT, coordinates IT purchases, and manages IT assets through their life cycles.

**a. IT Purchasing Management Branch (ASP-310):**

(1) Serves as the centralized source for the procurement of FAA IT related equipment, software, supplies, and services;

(2) Processes Procurement Requests (PR), Interagency Agreements (IAA), and Purchase Card (PC) transactions utilizing the FAA's Purchase Request Information System (PRISM) ensuring that the goods or services requested are received in a timely manner;

(3) Provides financial data and reports for the breakdown and analysis of IT spending; and

(4) Trains AIT staff on the use of the IT Acquisition Request system to initiate and track status of purchase requests.

**(a) IT Commodities Purchasing Section (ASP-311):**

i. Processes PC transactions utilizing the FAA's PRISM ensuring that the goods or services requested are received in a timely manner; and

ii. Reconciles PC transaction with the FAA's bank vendor to ensure accuracy and makes corrections as needed.

**b. Hardware Asset Management Branch (ASP-320):**

(1) Integrates financial, contractual logistic, and inventory functions to manage FAA IT assets, including hardware and peripherals;

(2) Reviews available options and assists with procurement planning and documentation;

(3) Develops and maintains policies, standards, processes, systems, and measurements to manage the IT asset portfolio with respect to risk, cost, governance, and performance objectives; and

(4) Manages reutilization of excess inventory, investigates lost equipment, and maintains a loaner pool of devices configured for international travel and/or contingency operations.

**c. Life Cycle Management Branch (ASP-330):**

(1) Concentrates on Life Cycle Management (LCM) for FAA IT assets, including hardware and peripherals;

(2) Maintains and tracks IT assets needs and manages asset replacements upgrades to maximize efficiencies and minimize costs; and

(3) Manages the disposal of IT equipment that is no longer required by the agency.

**6. Contract Management Support Services (ASP-400).** ASP-400 serves as CORs services division and provides day-to-day contract management support services for all the IT contracts, task orders, enterprise services contracts, IAA and FAA SAVES hardware contracts. This division provides coordination and approvals on applicable CIO requests and approval. ASP-400 provides support and guidance to customers and ensures appropriateness of the CIO package submission in accordance with the FAA AMS.

**a. Contract Services A Branch (ASP-410):**

(1) Works with the Contracting Officer (CO) on ratifications and changes to contracts, including Purchasing Requests (PRs) for new requests and for incremental funding for existing contracts;

(2) Provides assistance and oversight for the Project Manager's (PM's) development of the Statement of Work (SOW), Performance Work Statement (PWS), Statement of Objective (SOO), Independent Government Cost Estimate (IGCE), and IT Acquisition Requests (ITAR) which leads to a purchase or PR;

(3) Provides strategic and advisory services relative to acquisitions, IT service contracts, and makes recommendations to AIT management on the overall acquisition approach and contract type and/or vehicle that would deliver the best results;

(4) Evaluates existing contract portfolios, provides contract comparisons, analyzes business value, makes contract consolidation recommendations, and gathers vendor performance metrics; and

(5) Provides data support collection and reporting on IT acquisition activities and provides input for the acquisition roadmap for all the legacy and expiring contracts as AIT Contract Services moves forward with follow on agreements and/or contract/task orders.

**b. Contract Services B Branch (ASP-420):**

(1) Serves as the COR or Engineering Technical Officer (ETO) and provides day-to-day administration support of existing AIT contracts and task orders, including serving as ETO on multiple task orders under the National Airspace System (NAS) Integration Support Contract;

(2) Works with the CO on ratifications and changes to contracts, including PRs for new requests and for incremental funding for existing contracts;

(3) Provides assistance and oversight for the PM's development of the SOW, PWS, SOO, IGCE, and ITAR which leads to a purchase or PR;

(4) Provides strategic and advisory services relative to acquisitions, IT service contracts, vendor management, and makes recommendations to AIT management on the overall acquisition approach and contract type and/or vehicle that would deliver the best results;

(5) Evaluates existing contract portfolios, provides contract comparisons, analyzes business value, makes contract consolidation recommendations, and gathers vendor performance metrics;

(6) Provides data collection and reporting on IT acquisition activities and provides input for the acquisition roadmap for all the legacy and expiring contracts as AIT Services moves forward with follow-on agreements; and

(7) Provides due diligence and coordination with FAA organizations on requests for IT acquisitions subject to review and approval by the CIO in accordance with the FAA AMS.

**7. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 4. Enterprise Program Management Service (AEM)

## 1. Director of Enterprise Program Management Service (AEM-1).

### a. Roles and responsibilities:

(1) Has authority to make changes in AEM structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA IT policy and procedures as directed by the CIO;

(2) Organizes and manages resources to execute approved programs and projects;

(3) Ensures programs and projects are completed within the defined scope, quality, time, and cost constraints using consistent and defined standards;

(4) Enables informed decision making;

(5) Facilitates risk awareness and risk management;

(6) Manages and tracks the AIT portfolio of programs and projects to ensure everything is properly resourced, coordinated, and effectively run;

(7) Tracks FAA capital investments and reports on Exhibit 300 and Exhibit 53 items; and

(8) Provides Project Management resources for all AEM-100 – AEM-400 managed projects and programs:

**(a) IT Project Manager (IT PM)** is deployed when all Project Management Life Cycle (PMLC) documentation is required to support an IT Development Project that does not currently have a IT PM leading it (FED or Vendor CTR). Key required deliverables include a charter, project management plan/schedule, scope management plan, communications management plan, risk management plan, lessons learned, and project closure documentation;

**(b) Junior IT Project Manager** is deployed when some PMLC documentation is needed to facilitate the fulfillment of the task (e.g., schedule and/or requirements) or the effort requires an AIT employee to coordinate key tasks between/among/within a team(s) and /or organizations;

**(c) Task Coordinator** is deployed when no PMLC documentation is required or the effort requires an AIT employee to coordinate key tasks between/among/within a team(s) and/or organizations; and

**(d) AIT Liaison** is deployed when no PMLC documentation is required or the effort requires an AIT employee to represent a non-AIT LOB customer in obtaining information from AIT (e.g., in order to secure AIT resources, convey AIT requirements, etc.).

**b. Mission:** The Enterprise Program Management Service (EPMS) leads AIT's programs management, portfolio management, and program control services by applying defined standards to achieve strategic priorities.

**2. Operations Management Portfolio Division (AEM-100).**

a. Manages AIT's portfolio of operations-related programs and projects for Aviation Safety (AVS), Air Traffic Organization (ATO), Airports (ARP), and Commercial Space Transportation (AST);

b. Coordinates the creation and delivery of work products and deliverables;

c. Provides day-to-day management and oversight of the critical elements of programs and projects including budget, schedule, risk, and Earned Value Management (EVM) when applicable;

d. Works with the EPMS Management Team and other AIT Service Managers, and stakeholders to advance the EPMS service and AEM-100 goals and objects; and

e. Works closely with technical subject matter experts (SMEs) in other AIT Services to ensure projects are executed successfully.

**(1) Operations Management Portfolio A Branch (AEM-110):** Supports AVS, ATO, ARP and AST projects.

**(2) Operations Management Portfolio B Branch (AEM-120):** Supports AVS, ATO, ARP and AST projects.

**3. Unmanned Aircraft System (UAS) Program Office Division (AEM-200).**

a. Manages AIT's portfolio of UAS-related projects;

b. Coordinates the creation and delivery of work products and deliverables;

c. Provides day-to-day management and oversight of the critical elements of programs and projects including budget, schedule, risk, and EVM when applicable; and

d. Works closely with technical SMEs in other AIT Services to ensure projects are executed successfully.

**(1) Unmanned Aircraft System (UAS) A Branch (AEM-210):** Supports AVS and ATO projects related to UAS.

**4. Business Management Portfolio Division (AEM-300):**

a. Manages AIT's portfolio of business-related projects;

b. Coordinates the creation and delivery of work products and deliverables;

c. Provides day-to-day management and oversight of the critical elements of programs and projects including budget, schedule, risk, and EVM when applicable; and

d. Works closely with technical SMEs in other AIT Services to ensure projects are executed successfully.

**(1) Business Management Portfolio A Branch (AEM-310):** Supports AFN and AHR projects.

**(2) Business Management Portfolio B Branch (AEM-320):** Supports Office of Audit and Evaluation (AAE), AHR and AIT projects.

**5. Enterprise Management Portfolio Division (AEM-400).**

a. Manages AIT's portfolio of enterprise-wide projects for AIT and FAA services;

b. Coordinates the creation and delivery of work products and deliverables;

c. Provides day-to-day management and oversight of the critical elements of programs and projects including budget, schedule, risk, and EVM when applicable; and

d. Works closely with technical SMEs in other AIT Services to ensure projects are executed successfully.

**(1) Enterprise Management Portfolio A Branch (AEM-410):** Supports AIT projects.

**(2) Enterprise Management Portfolio B Branch (AEM-420):** Supports AIT projects.

**6. Performance, Planning & Program Control Division (AEM-500).**

a. Manages and tracks the AIT portfolio of programs and projects to ensure that it is properly resourced, coordinated, and effectively run; and

b. Tracks FAA Capital Investments and reports on Exhibit 300 and Exhibit 53 items.

**(1) Budget, Program Control & Capital Planning & Investment Control (CPIC) Branch (AEM-510):**

(a) Concentrates on the resources of EPMS, including financial and human resources, estimates costs and develops budgets for EPMS programs and projects;

(b) Tracks and secures funding from FAA customers for respective Project Level Agreements;

(c) Supports the AIT Intake process and assists EPMS leadership with resource management, to enable the organization to focus resources where most needed; and

(d) Tracks and reports on the IT portfolio of investments to meet CPIC requirements, including Agency IT Portfolio Summary, Agency Cloud Spending Summary, Major IT Business Case and Major IT Business Case Detail.

**(2) Planning Reporting & Risk Branch (AEM-530):**

(a) Supports EPMS's business planning efforts, and reports on EPMS's portion of the AIT Business Plan;

(b) Manages tools used to track the progression of programs and projects throughout the Program Management Lifecycle and assists EPMS leadership manage all aspects of the portfolio;

(c) Manages EPMS's Integrated Master Schedule;

(d) Promotes project management methodology and best practices, provides training and opportunities to enhance PM skills and shares knowledge via Community of Practice sessions;

(e) Highlights risk within AIT's portfolio of programs and projects, and provides EPMS leadership with the necessary information to make risk aware decisions; and

(f) Provides risk management training, consulting, and gates to identify, assess, manage, monitor, and report IT risks.

**7. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 5. Business Partnership Service (APS)

## 1. Director of Business Partnership Service (APS-1).

### a. Roles and responsibilities:

(1) Has authority to make changes in APS structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA IT policy and procedures as directed by the CIO;

(2) Business Partnership Service (BPS) is responsible for enterprise-wide stakeholder relationship management. As the front door into IT and serving as the liaison for FAA business stakeholders who need IT support, BPS interacts with stakeholders to ensure their needs are met. BPS develops and maintains stakeholder relationships, as well as collaborates, and provides technical solutions;

(3) BPS provides the primary interaction with IT stakeholders to understand their needs, foster collaborative solutions, and build credibility as a trusted partner. BPS is responsible for the end-to-end stakeholder relationship management process;

(4) BPS oversees and manages the MyIT Service Center, a centralized, single POC for IT related incidents, inquiries and service requests. The MyIT Service Center is the FAA's 24x7 IT helpdesk, to provide support and quickly resolve stakeholder IT issues, requests and questions; and

(5) BPS maintains the AIT Service Catalog, the central location for stakeholders to fulfill their standard IT needs.

### b. Mission:

(1) Relationships: Fosters a collaborative and unifying culture fueled by communication and outreach;

(2) Responsive: Understands stakeholder business needs and connects them with options and solutions;

(3) Service: Employees are professional, courteous, respectful, and promote a sense of community;

(4) Trust and value: Trusted advisors in strategic initiatives with our business partners; and

(5) Change agents: Continually drives change to ensure a peak stakeholder experience.

## 2. Intake & Portfolio Management Staff Office (APS-010):

a. APS-010 is the front door for all external stakeholder requests. This Team is responsible for gathering, recording and tracking stakeholder requests coming into AIT and routing requests

appropriately for rapid fulfillment. APS-010 provides executive level metrics and dashboards to AIT leadership on incoming requests from stakeholders and their status; and

b. APS-010 is responsible for coordinating and facilitating periodic reviews with stakeholder. APS-010 works collaboratively with the AIT verticals to develop executive level briefings for stakeholder organizations focused on their current information technology activities, future information technology activities, portfolio management and critical issues. Portfolio reviews are used to highlight upcoming AIT initiatives, and address questions and concerns from the stakeholder LOB.

**3. Business Partnership Management (BPM) Division (APS-100).**

a. Provides and fosters the relationships between FAA business units and the IT organization as a trusted business partners;

b. Serves as one of the three 'front doors' to IT providing the primary interaction with LOBs to understand their needs. Key roles that support this mission are BPMs and Business Partnership Representatives; and

c. Promotes, on a daily basis, IT programs and projects to their stakeholders, intervenes to resolve issues before they become critical, and maintains collaborative relationships across AIT.

**(1) Business Partnership Management A Branch (APS-110):**

(a) Represents the Business Unit's interest within the broader IT Shared Services Organization;

(b) Serves as account managers for IT requests and helps ensure business unit needs flow through the AIT organizational units; and

(c) Supports ATO, AFN, AHR, Regions and Property Operations, and AIT itself.

**(2) Business Partnership Management B Branch (APS-120):**

(a) Represents the Business Unit's interest within the broader IT Shared Services Organization;

(b) Serves as account managers for IT requests and helps ensure business unit needs flow through the AIT organizational units; and

(c) Supports AVS, AST, Office of Security and Office of Security and Hazardous Materials Safety, NexGen and ARP.

**(3) Business Partnership Management C Branch (APS-130):**

(a) Represents the Business Unit's interest within the broader IT Shared Services Organization;

(b) Serves as account managers for IT requests and helps ensure business unit needs flow through the AIT organizational units; and

(c) Supports the AAE, Office of the Chief Council, Office of Government and Industry Affairs, Office of the Administrator, Office of Communications (AOC), Office of Civil Rights, and Office of Policy, International Affairs & Environment.

**4. Customer Support Services Division (APS-200)** manages the AIT Service Catalog and all activities.

**a. Service Catalog Branch (APS-210):**

(1) Manages the AIT Service Catalog, known as MyIT Services, a resource for all FAA employees to find and learn more about the IT services and products offered by AIT;

(2) Regularly monitors, analyzes, and reports on services delivered within the catalog;

(3) Ensures that the IT workforce is knowledgeable about IT capabilities and services that are available to the business; and

(4) Works with Service Owners within AIT to develop and improve the process and workflows for MyIT Services to be delivered to FAA employees.

**b. Customer Experience & Innovation Branch (APS-220):**

(1) Provides solutions that enhances the user experience of FAA employees for products and services that are provided from AIT;

(2) Collaborates with product owners within AIT to understand the product and services deployed to FAA users and identify the changes that impacts the stakeholders experience;

(3) Coordinates the development of material as needed to enhances the overall experience of FAA users;

(4) Provides guidance and content to the stakeholder outreach initiatives, such as the Service Concierge, to answer user questions and provide information to enable the optimal user experience;

**5. Service Center Division (APS-300)** serves as a central POC between FAA users and IT service management providing support for restoration of services, handling of new service requests, providing status of incidents.

**a. Service Delivery and Operations Branch (APS-310):**

(1) Provides management and oversight of the FAA helpdesk;

(2) Develops, validates, and integrates processes, provides technical and policy guidance, manages the escalation process, and enables self-service tools; and

(3) Identify, streamline, and implement IT processes to improve overall stakeholder experiences.

**b. Helpdesk Operations Section (APS-311):**

(1) Provides day-to-day oversight of service center operations worldwide. Coordination of daily operations, tracking of all MyIT Service Center requests via regular and ad-hoc reporting, escalations and integration of new functions from IT and non-IT support;

(2) Directs support staff to follow Information Technology Infrastructure Library (ITIL) related processes: Incident Management, Knowledge Management, Problem Management, and Release Management processes for a consistent improved stakeholder experience. Provides feedback and input to continually improve the ITIL related processes;

(3) Provides 24x7 after-hours escalation support and coordination with Tier 2 and Tier 3 teams. Notifies AIT Leadership of escalated outages as appropriate;

(4) Provides management and oversight of the ATO Tech Ops Maintenance Display Terminals (MDTs), support and coordination for hardware LCM, local FAA facility activities, and special projects tools;

(5) Oversees escalation management along with the self-service tools available. Provides reporting of all incident/request related data sets including helpdesk calls, incidents, requests, outages, projects and trend analysis.

**c. Project Implementation Section (APS-312):**

(1) Provides management and oversight of the ATO Tech Ops MDTs, and supports the coordination for hardware LCM, local FAA facility activities, and special projects which require support from the Service Center Operations group; and

(2) Provides coordination on AIT projects when impact and implementation requires remote or onsite support for the service center contractors. This can include coordination for software and hardware install, infrastructure related support, asset management actions, break/fix, LCM, offsite events (Sun-n-fun, Oshkosh, etc.) and associated project related activities.

**6. Strategic Service Management Office (APS-400):** Strategically administers, manages, and oversees the delivery of enterprise IT support services resulting in an improved stakeholder experience and increased overall stakeholder satisfaction.

**a. Contract & Financial Management Branch (APS-410)** provides contract oversight for assigned strategies contract. Handling the review and approval of all contract required deliverables.

**b. Service Assurance & Performance Branch (APS-420)**

(1) Manages Incidents, Knowledge and Problem Management programs;

(2) Provides Quality Assurance and Service Level metric analysis, Information Technology Service Management and Remote tools support, and the product catalog used for data categorization; and

(3) Provides detailed reporting and analysis of the assigned strategic contracts.

**7. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 6. Solution Delivery Service (ADE)

**1. Director of Solution Delivery Service (ADE-1).**

**a. Roles and responsibilities:**

(1) Has authority to make changes in ADE structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA and Cybersecurity and Privacy policy and procedures as directed by the CIO;

(2) Provides application development and sustainment services, with an emphasis on the design, development and support of technical solutions, to meet and exceed the needs of IT customers; and

(3) Provides quality management, collaboration, middleware, and database administration services that support IT customers.

**b. Mission:** ADE provides technical expertise and develops innovative products and services to solve complex challenges facing AIT's business partners. From quality management and testing, technology standards and roadmaps, enterprise collaboration and middleware services, to database administration and DevSecOps toolchain services to application development and sustainment, ADE delivers. ADE is committed to designing new and innovative ways to leverage the FAA cloud and works closely with AIT's business partners in areas such as collaboration, mobility, and citizen development.

**2. Business Operations (ADE-010).** ADE-010 serves as the "front door" to Solution Delivery.

a. Tracks and monitors work assigned, manages the demand for resources and the total cost to the taxpayer model for supported applications. ADE-010 manages the business of ADE including budget, financial planning, data calls, business planning, processes, training strategy, and the SD Landing Page;

b. Provides a comprehensive understanding of the work of ADE. This staff office has visibility into all activities and projects across the organization, and understands the pipeline of inbound work. ADE-010 oversees the Solutions Work Assessment Team, ensuring the efficient intake of work. ADE-010 leads capacity planning and works closely with the AIT Intake Staff Office to provide the appropriate staffing resources to support the execution of AIT's programs and projects;

c. Manages the contract strategy for ADE moving toward flexibility and resource scalability by demand;

d. Ensures ADE processes are documented, maintained, and accessible to employees. ADE-010 serves as a liaison between the process authors within ADE's Divisions and ASP for process development, coordination, and related activities;

e. Manages ADE business and strategic planning, data calls, awards, staffing, training strategy and the SD Landing Page. Provides administrative support and oversight for ADE directorate; and

f. Manages ADE financials, agreements, total cost to taxpayer for ADE supported applications, and provides data for ADE leadership to make decisions.

**3. Quality Management & Planning Division (ADE-100).** ADE-100 ensures products are suitable for their intended purpose, meet requirements, and operate to customer expectations.

**a. Quality Assurance Branch (ADE-110):**

(1) Promotes a "Quality First' culture with built-in security through various collaborative, security, and quality-driven initiatives;

(2) Provides Quality standards guidance, Software Development Life Cycle quality checks, and quality audits; tracks compliance and reports; oversees lessons learned and process improvement; and

(3) Holds Quality Forums regularly; advances Robotics Process Automation capabilities; and ensures accessibility and Section 508 compliance, as required.

**b. Quality Operations Branch (ADE-120):**

(1) Ensures that ADE products are suitable for their intended purposes, meet all agreed to requirements, are implemented securely per FAA cybersecurity and privacy requirements, and operates to customer expectations;

(2) Supports the creation of the Program Requirements and the Requirements Definition Guidelines documents required for Joint Resources Council/AMS investments, ensures cybersecurity and privacy requirements are included, and the team reviews proposed changes to AMS policy that relate to these documents;

(3) Work in cross-functional teams to plan, prioritize, and deliver information architecture, information design, visual design/page layouts, tools, services, and applications to support a cohesive user experience. The team leverages modern web technologies to define innovative user interfaces and interactions models that result in improved productivity and operational efficiency, and educate project teams about best practices;

(4) Designs, plans, and coordinates solution quality to identify the business value and ensure those requirements are met;

(5) Works with PMs on Quality Management/Assurance and Test Planning/Management, ensuring the solution formally identifies and follow software development methodology, meets standards and is suitable for its intended purpose and works correctly; and

(6) Oversees test execution, including functional, regression, user acceptance interface/system, compatibility, and performance/load and accessibility testing.

**4. Solution Strategy Division (ADE-200).** Designs solutions that effectively use data and align to the goals, processes, and security standards within AIT and the FAA.

**a. Enterprise Architecture Branch (ADE-210):**

(1) Supports the Branch in meeting its strategic objectives by employing its internal Technical Analysis Investment Team;

(2) Collects, connects, and relates data and information to assist management in making informed strategic decisions to achieve future-state goals. Enterprise Architecture (EA) is a management practice for aligning resources to improve business performance and help the FAA better execute its core mission. EA describes the current and future state of the agency, and lays out a plan for transitioning from the current state to that future state; and

(3) Facilitates and supports a common understanding of business needs, helps formulate recommendations to meet those needs, and facilitates the development of a plan of action that is grounded in an integrated view of technology planning, mission/business planning, capital planning, security planning, infrastructure planning, human capital planning, performance planning, and records planning. EA focuses on the FAA's information, infrastructure, applications, and performance architectural domains.

**b. Discovery Services Section (ADE-211):**

(1) In coordination with BPMs and customers, this section supports AIT Work Intake by providing high-quality and realistic proposals that offer innovative solution options for meeting customer needs; and

(2) Discovery Services is tightly aligned with the Enterprise Architecture Branch and furthers the mission of technology planning to drive transition to future state technologies.

**c. Product and Portfolio Management Branch (ADE-220):**

(1) Provides product portfolio management for all AIT/ADE supported software products by maintaining a "living" product roadmap;

(2) Tracks all software products to ensure they are delivered, maintained, and sunsetted appropriately, and meet the needs of system owners;

(3) Works with AIT PMs, DevOps Leads, Sustainment Leads, BPMs, Enterprise Architects, Security Engineers and others to have the latest information on current and future improvements for the software product roadmap;

(4) Captures risks associated with software products in terms of security, finance, technology, or business related impacts;

(5) Ensures technology solutions align to business goals, follows approved processes, uses enterprise information in a consistent manner, integrates effectively with other applications, supports a common application environment and user interaction model, uses a common technology platform, and achieves enterprise-level security and scale;

(6) Works closely with the Solution Architecture and EA Teams to ensure alignment with AIT standards while planning future technological capabilities;

(7) Helps AIT hone in on technologies that will be useful to the FAA in the future by employing the Research & Innovation team and conducts proof of technology and proof of concept research; and

(8) Provides technology platforms for Enterprise Search services by making structured and unstructured enterprise content easy to find through indexing and retrieval.

Works closely with the Solution Architecture and EA teams to ensure alignment with AIT standards while planning future technological capabilities;

**d. Solution Architecture Branch (ADE-230):**

(1) Responsible for the logical and physical design of web applications;

(2) Oversees and manages the conceptualization, detailed design, and development of technology solutions;

(3) Concentrates on the definition and description of the architecture of a system delivered in context of a specific solution, and as such, it may encompass an entire system or a specific part of that system;

(4) Provides oversight into the development of application-level code and processes within the application development environment, including integration of new and existing functionality; and

(5) Ensures that delivered solutions are of a consistently high quality, are delivered against a clear and stable set of requirements, moves the IT architecture forward, and are operationally fit.

**5. Enterprise Information Services Division (ADE-300).** Provides technology platforms to enable FAA employees and stakeholders to work collaboratively.

**a. Enterprise Collaboration & Document Management Services Branch (ADE-310):**

(1) Provides a variety of consultative capabilities and technology platforms that enable FAA employees to work collaboratively;

(2) Understands how people collaborate in the context of geographically distributed and ad-hoc teams, on-premises and mobile work environments, and how they work together to use, develop, and apply content to business needs;

(3) Recognizes the “community” as the application, empowering users to solve problems for themselves and apply the right tools to the difficulty in any situations;

(4) Responsible for the Knowledge Services Network, collaboration projects, www.faa.gov, my.faa.gov, and their supporting search and content management systems; and

(5) Provides technology platforms and advisory services for enterprise document and content management services.

**b. Data Integration Services Branch (ADE-320):**

(1) Supports integration services including Service Oriented Architecture (SOA), operational web services, Application Program Interfaces (API) and data virtualization; and

(2) Provides technology platforms and advisory services for enterprise integration services, which promote reuse via enterprise standards and frameworks, supports integration services including SOA, operational web services, API management and data virtualization.

**c. Identity & Access Management Services Branch (ADE-330).** Supports the MyAccess platform which provides the FAA Identity and Access Management service;

**6. Application Data Services Division (ADE-400).** Includes Software & Tools Management and Database Management.

**a. Software & Tools Management Branch (ADE-410):**

(1) Manages the "middle-tier" architecture for effective software development, as well as the reading and writing of data to create applications;

(2) Responsible for the web platforms and tools that AIT developers use to build software;

(3) Manages application servers, oversees the test and production environments, and supports deployments from one environment to another;

(4) Supports numerous custom web applications running on Internet Information Service, TomCat, SharePoint, WebSphere, ColdFusioon, and BPM platforms; and

(5) Automates deployments using DevSecOps methodologies, which will streamline AIT's deployment of applications to the cloud.

**b. Database Management Branch (AE-420):**

(1) Responsible for the maintenance and security of data and databases attached to FAA applications in AIT's production environments; and

(2) Installs, configures upgrades, administers, monitors, and maintains a vast number of FAA databases.

**7. Solution Operations Division (ADE-500).** Includes application sustainment, enhancements and system security compliance support.

**a. Solution Operations A Branch (ADE-510):** Serves as developers and sustainment coordinators. Their responsibilities are described below (Section 6, Paragraph 7 c.).

**b. Solution Operations B Branch (ADE-520):** Serves as developers and sustainment coordinators. Their responsibilities are described (Section 6, Paragraph 7 c.).

**c. Solution Operations C Branch (ADE-530):** Serves as developers and sustainment coordinators. Their responsibilities are described below.

(1) Solution Operations A, B, and C Branches manage business applications in AIT's production portfolio;

(2) Oversees the operations, break/fix, maintenance, environment upgrades, small customer requests, and system administration of the applications that are in AIT's production environment;

(3) Works closely with ADE's Product Managers to manages the overall health of each application specifically ensuring that it is available, technically viable, secure, and has current documentation; and

(4) Provide Tier 3 support to applications.

**8. Organizational Chart**. The organization chart is available on the MyFAA employee website**:** https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 7. Infrastructure & Operations Service (AIF)

## 1. Director of Infrastructure & Operations Service (AIF-001).

### a. Roles and responsibilities:

(1) Has authority to make changes in AIF structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA IT policy and procedures as directed by the CIO;

(2) Directs, manages and maintains FAA Mission Support and IT test and production environments, protects from harm and re-establishes operations when a detrimental event occurs; and

(3) Manages and maintains the foundation of all FAA non-NAS IT networks, IT infrastructure, and IT data centers.

**b. Mission:** AIF manages AIT's operational environments and protects them from harm. The organization provides a wide array of services, ranging from planning, design, testing, transition and operation support in the production environment. Delivering effective back-end solutions, to monitor the integrity and optimization of the operation of the agency's networks, data centers, and applications, AIF ensures that the FAA runs an effective and efficient infrastructure.

## 2. FAA Cloud Services (FCS) Special Program Office (SPO) (AIF-001).

a. The mission of the FAA FCS SPO is to provide an enterprise solution for agency cloud computing needs. AIF-001 provides a full scope of program management support, including contract management, program control, and stakeholder management;

b. Services cloud architecture needs by building and refining cloud architecture, developing implementation strategies, and coordinating change effectively across the enterprise;

c. Manages migration of applications to the cloud, by conducting cloud suitability assessments, planning for capacity, and coordinating migrations; and

d. Provides a full lifecycle of operational support, to include governance, implementation, delivery orders, quality assurance, and incident response.

## 3. Enterprise Operations Center (AIF-010).

a. The Enterprise Operations Center's (EOC) mission is to provide automated 24x7 monitoring, alerting, services performance, reliability and optimization for systems, services and infrastructure in the FAA. Use predictive analysis methods to anticipate issues before they occur, reduce service interruptions, and maximize service uptime. EOC also provides live monitoring, AIF communications and troubleshooting for IT Services interruptions from 7am to 6pm, Monday through Friday;

b. Through continuous monitoring, AIF identifies interruptions to systems and service as soon as they occur;

c. Facilitates root cause analysis, and coordinates response efforts with other AIT organizations to ensure service is restored in a timely manner. EOC initiates service interruption notices and other communication to AIT stakeholders; and

d. Manages several enterprise tools used to monitor, alert and trend application and network performance and availability, facilitates and conducts problem and Tiger Team troubleshooting sessions to resolve more complex issues.

**4. Performance & Planning Division (AIF-100).**

a. Serves as the front-door to the AIF organization; and

b. Provides centralized infrastructure and operations planning, design, performance tracking, AIF-specific project management and integration services to promote effective and efficient operations.

**(1) Performance & Reporting Branch (AIF-110):**

(a) Establishes, monitors, and reports on overall metrics and performance targets for AIF. AIF-110 is responsible for collecting and analyzing baseline vs. current performance data on network and server performance, conducting impact analysis, and providing information in response to data calls; and

(b) Serves as an authoritative source for AIF data inquiries, performance and trending; assists in reporting and gathering data for all agency data calls.

**(2) Infrastructure & Operations Project & Resource Management Branch (AIF-120):**

(a) Oversees capacity planning, work intake, project management, incident management, and workforce management. Provides the single view of the current workload of the AIF organization, tracking all work initiatives, coordinating resource assignment and project planning, and tracking the overall utilization and availability of AIF resources;

(b) Manages AIF's work intake. AIF-120 uses standard processes to accept, assess, review, assign, and track Service Requests. They provide insight to AIF leadership on workload levels and recommendations on resource availability and prioritization of work. AIF-120 provides input into the portfolio planning process and coordinates inputs into Service Level Agreements;

(c) Supports the management of customer incidents originating from the MyIT Service Center and other sources. AIF-120 provides monitoring, initial assessments, accurate and timely assignments, and standard reporting services for restoration and request incidents received from customers; and

(d) Provides project management support for projects and initiatives specific to AIF. AIF-120 collaborates with AIF management to identify appropriate project leads to execute identified infrastructure projects, and ensures that AIF has the required project management resources available. AIF-120 coordinates with AIT work intake teams as well as EPMS in the delivery of enterprise projects, and manages and tracks said projects.

**(3) Network & Data Center Planning & Design Branch (AIF-130):**

(a) Collaborates within AIF and across the AIT Services to design and implement new network and data center technologies and configurations;

(b) Fulfills requests to lead or participate in network, data center, and infrastructure services projects. AIF-130 provides the business case for testing and implementing new technology and, once approved by management, initiates projects related to the new technology. AIF-130 forecasts the project budget, sets priorities, analyzes project risks and constraints, and manages resources to best achieve the project goals; and

(c) Architects, configures, and implements the hardware required to operate networks (Local Area Network (LAN)/Wide Area network (WAN)) and data centers, in coordination with AIF's Operations Services Division. AIF-130 plans, designs, and manages the lifecycle of network and data center topologies and configurations, and sets and documents standards for network and data center technologies. AIF-130 provides network and data center guidance to facilities that are new, moving, or renovating and coordinates the installation of new network circuits.

**(4) Client Planning & Design Branch (AIF-140):**

(a) Collaborates within AIF and across the AIT Services to plan for and design new client technologies and configurations;

(b) Fulfills requests to lead or participate in client related projects. AIF-140 provides the business case for testing and implementing new technology and, once approved by management, initiates projects related to the new technology. AIF-140 forecasts the project budget, set priorities, analyzes project risks and constraints, and manages resources to best achieve the project goals; and

(c) Develops the roadmap for the continuing evolution of the client in coordination with ADE's Enterprise Architecture Branch, S&P's Asset Management Branches, and BPS's Business Partnership Management Division. In coordination with AIF's Client Integration and Testing Branch, architects hardware and software required to operate the FAA client. AIF-140 assists with building the client image(s), planning and designing the lifecycle of client topologies and configurations, and sets and documents standards for client technologies.

**5. Transition Services Division (AIF-200):** Provides comprehensive management and oversight of AIT's test and production environments. AIF-200 manages the transition process from test to production and is responsible for the planning, scheduling, bundling, releasing, and tracking of all changes.

**a. Enterprise Change & Configuration Branch (AIF-210):**

(1) Manages AIT's Enterprise Change Management Process, and focuses on the efficient, effective, and comprehensive management of all changes to the IT production environment;

(2) Utilizes standardized methods and procedures to promptly handle all requests for changes to the IT production environment in order to minimize the number and impact of related incidents on service. AIF-210 is responsible for receiving, logging, prioritizing, and facilitating the completion of all change requests. This includes updates the change log with all progress as it occurs, closes requests for completed changes, and provides reports to management on all changes to the IT production environment;

(3) Chairs AIT's Enterprise Change Management Board. The AIT Enterprise Change Management Board assesses, approves and authorizes for implementation changes to the IT Production Environment; and

(4) As the Librarian of all configuration items, works closely with Asset Management to ensure AIT has a clear picture of all hardware, software, and supporting assets that are in the FAA's IT production environment. AIF-210 manages the Configuration Management Database (CMDB) tool.

**b. Release Branch (AIF-220):**

(1) Protects the integrity of the FAA's IT production environment by effectively planning, scheduling, communicating, and deploying releases from the test environment to the live production environment;

(2) Ensures that releases are clearly defined and successfully transitioned into production. AIF-220 conducts a final readiness review on all new solutions, client configurations, patches, equipment, and any other changes to the IT production environment. After deployment to the production environment, AIF-220 verifies the success of the deployment, and provides regular metrics and reports to AIF management; and

(3) Takes an active role in assisting with the installation and deployment of hardware into the production environment. AIF-220 assists AIF's operational branches to perform assigned functions by traveling to a location, installing, replacing, and in some cases configuring hardware. They interact with AIF's Client Planning & Design Branch, and AIF's Client Integration & Testing Branch, to ensure operability and successful deployments and installations on client endpoints. Manages and maintains the Mobile Device Management software (currently AirWatch).

**c. Pre-Production Environment Management Branch (AIF-230):**

(1) Builds, documents, and manages test environments to support the transition of solutions into the IT production environment; and

(2) Builds both Client and Isolated System test environments that simulate multiple facets of the IT production environment including, but not limited to, applications, Group Policy Objects (GPO), client images, and patching.

**d. Client Integration & Testing Branch (AIF-240):**

(1) Collaborates with members of the Client Planning & Design Branch to test and implement new hardware and software client technologies; and

(2) Responsible for patching clients, managing all aspects of Group Policies and scripts, implementing client baseline configurations, packaging applications that require changes to the client, testing changes to clients, and managing the client portion of the Pre-Production Environment. In conjunction with AIF-220, manages, configures and sets standards for Mobile Devices including, but not limited to, iOS version, iTunes version, and configuration of Mobile Devices.

**6. Operations Services Division (AIF-300).** Responsible for the health of the overall operational environment. They manage the effective execution of IT operations, and the delivery of infrastructure services including directory and account management services, network operations, data center services, and infrastructure applications.

**a. The Directory Services Branch (AIF-310):**

(1) Administers and monitors the Mission Support authentication systems and services. Troubleshoots and resolves associated service degradations and outages;

(2) Makes updates to directory services based on applications, patches and security needs;

(3) Provides escalated IP address management, name resolution and group policy technical support;

(4) Creates and manages trusts and administers the Active Directory Private Key Infrastructure for the Mission Support environment to allow for resource access and Personal Identity Verifications (PIV) or Common Access card; and

(5) Works closely with Security Operation Center (SOC) to assist with and provide information for security incidents

**(a) Account Management Section (AIF-311):** As part of the Directory Services Branch, this branch:

i. Authenticates and organizes user accounts and services on the FAA network;

ii. Oversees the effective delivery of directory and account management services, designates and enforces access rights across the network, tracks and updates individual and group directory accounts, establishes policies and standards for individual and group objects, and makes updates to directory services based on patches and security needs; and

iii. Creates test accounts, creates groups, runs Lightweight Directory Access Protocol queries, and helps integrate PIV in the FAA environment.

**b. Network Services Branch (AIF-320):**

(1) Enables the successful operation of the FAA's network systems and services including LANs, WANs and Trusted Internet Connections (TICs). AIF-320 administers, configures, manages, and troubleshoots the infrastructure that protects the FAA's network, including firewalls, switches and routers, Network Access Control (NAC), wireless, Bluecoat, BlueCat, IronPort, and BlackHole; and

(2) Maintains availability of network services and work closely with the Network & Data Center Planning & Design Branch to schedule and implement updates to all network services. AIF-320 detects, diagnoses, troubleshoots, and resolves all network services outages and performance issues as they are identified.

**(a) Network Services B Section (AIF-321):**

i. Enables the successful operation of the FAA's network systems and services including LANs, WANs, and TICs. AIF-321 administers, configures, manages, and troubleshoots the infrastructure that protects the FAA's network, including firewalls, switches and routers, NAC, wireless, Bluecoat, BlueCat, IronPort, and BlackHole; and

ii. Maintains availability of network services and works closely with the Network & Data Center Planning & Design Branch to schedule and implement updates to all network services. AIF-321 detects, diagnoses, troubleshoots, and resolves all network services outages and performance issues as they are identified.

**c. Data Center Services Branch (AIF-330):**

(1) Manages the provisioning of hosting solutions for AIT's customers at the FAA's data centers, located in FAA Headquarters, the William J. Hughes Technical Center, and the Mike Monroney Aeronautical Center, as well as FAA Cloud Services. AIF-330 supports hosting file share resources for FAA field shares; and

(2) Responsible for managing AIT's operating systems, servers, virtual infrastructure, storage and backup solutions, and the F5 environment for load balancing application servers. AIF-330 provides environmental (space, power, cooling) hosting within the data centers, provisions the infrastructure to support web hosting, and configures the operating system environment for system disaster recovery solutions. AIF-330 provides engineering support services to system owners to develop high efficiency, resilient hardware solutions.

**d. Infrastructure Applications Branch (AIF-340):**

(1) Responsible for the operation and management of enterprise FAA business services, including but not limited to: Video Tele- Conferencing services, Endpoint Protection services, and Messaging operations services;

(2) Responsible for the system administration and operation of the MDM system, which enables easy and secure access to FAA network resources for approximately 5,000 government-furnished mobile devices and implements configuration settings to ensure the security of managed devices when connected to the FAA network;

(3) Provides second and third-tier level support for the FAA's room-based video conferencing systems, and software licenses for the mobile and desktop video conferencing application. AIF-340 provides consulting support on audio visual projects across the agency, from single room implementations through multipurpose conference centers with flexible space considerations; and

(4) Responsible for the system administration and operation of the agency's anti-virus and full disk encryption McAfee application suite, which provides protection to FAA's non-NAS network systems. AIF-340 implements configuration settings to ensure the security and protection of these systems.

**(a) Messaging Operations Services Section (AIF-341):**

i. Responsible for the system administration and operation of the FAA's Microsoft Office cloud messaging service;

ii. Supports accounts that provide email, instant messaging, and e-archiving services;

iii. Provides support services including e-discovery, integration with external business applications, and set-up of enterprise-wide broadcast announcements; and

iv. Maintains an instance of the legacy Lotus Notes application to support e-discovery requests.

**7. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 8. Information Security and Privacy Services (AIS)

## 1. Director of Information Security and Privacy Service (AIS-001).

### a. Roles and responsibilities:

(1) Has authority to make changes in AIS structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, authority to enforce changes in FAA IT policy and procedures as directed by the CIO. All other authorities, roles, and responsibilities as documented in the current edition of FAA Order 1370.121, FAA Information Security and Privacy Program & Policy;

(2) Performs the operational day-to-day activities intended to mitigate information security and privacy risks at the technical level;

(3) Develops and delivers IT security policy, architecture, standards, best practices, and privacy management for the FAA; and

(4) Ensures the security of the IT environment is compliant with FAA, DOT and Federal requirements; and

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

### c. Major Functions:

(1) Performs the role of the Chief Information Security Officer (CISO) as specified in FAA Order 1370.121;

(2) Responsible for developing, issuing, updating, and carrying out the FAA Enterprise Information Systems Security and Privacy Program;

(3) CISO serves as the chair of the Cybersecurity Steering Committee (CSC). The CSC is the Risk Executive for the FAA; and

(4) CISO advises the Risk Executive (i.e. CSC) of risk acceptance disagreements between the CISO and Authorizing Official.

**d. Functional Organization:** Information Security and Privacy Services.

**e. Delegations:** The Information Security and Privacy Service Deputy Director.

**f. Line of Succession:** The Information Security and Privacy Service Deputy Director. AIT-1 will determine line of succession if AIS -1 or AIS-2 cannot fulfill their duties.

**2. Chief Privacy Office (AIS-010):**

a. Provides expertise and oversight for privacy requirements across the FAA. AIS-10 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;

b. Manages the Identity Monitoring Code issuance process, responds to FAA privacy incidents, and oversees the handling of privacy requests, appeals, and complaints. AIS-10 supports teams within IS&P who are performing privacy risk assessments, PTAs, privacy awareness training, writing policy, PIAs, privacy audits and privacy audit tracking;

c. Provides guidance for the protection of Personally Identifiable Information (PII) and privacy records. AIS-10 works with stakeholders throughout AIT, FAA and DOT to ensure privacy requirements are met, and provides guidance for contact language involving privacy data; and

d. Works closely with the SOC on information security incidents involving privacy data, and works closely with AOC during privacy incidents that generate media interest.

**3. Security & Privacy Risk Management Staff (AIS-020):**

a. Projects the Social Security Number Reduction Plan security/privacy.

b. Manages the security dashboard and reporting mechanisms that support communication of the current state of security and privacy of the enterprise; and

c. 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. AIS-20 establishes and communicates the security and privacy risk tolerance of the enterprise in the form of policies, and performs periodic security and privacy risk assessments for the enterprise to ensure risk mitigations are in place and tolerance is being met. Works with security architects to develop and implement solutions that meet the risk tolerance while achieving business goals.

**4. Aviation Ecosystem Stakeholder Engagement (AIS-030):**

a. Provides security to the enterprise by strengthening the security of the aviation ecosystem through our collaboration with public and private entities, including the intelligence community. Systematically establish long-term engagements both internally and with external aviation ecosystem stakeholders by collaborating with key ecosystem entities (e.g. groups, organizations, manufacturers) and establishing engagement and participation in aviation ecosystem information exchange;

(1) Establish relationships with Aircraft Stakeholders for long-term engagement;

(2) Establish relationships with Airlines and Airlift Stakeholders for long-term engagement;

(3) Establish relationships with Airports Stakeholders for long-term engagement;

(4) Establish relationships with Aviation Management Stakeholders for long-term engagement; and

(5) Establish relationships with International Stakeholders for long-term engagement.

b. Understands aviation ecosystem cybersecurity risks and collaborate with stakeholders to enable improved resiliency. Enabling a cyber-secure and resilient aviation ecosystem as a trusted partner within FAA for strategic cyber stakeholder engagement. Engage in information sharing in support of aviation ecosystem cybersecurity improvement by participating in discussions, forums, conferences, etc.

c. Builds and maintains relationships with, and provide guidance to, external partners in Government and industry to sustain and improve cybersecurity in the Aviation Ecosystem. Identify, assess and analyze cyber threats, vulnerabilities, and consequences within the Aviation Ecosystem through support of research, development, testing, and evaluation initiatives, engage with Aviation Ecosystem stakeholders on activities for reducing cyber risks, and seek potential improvement opportunities and risk mitigation strategies.

(1) Rulemaking and standards development support;

(2) R&D Support; and

(3) Support for the interagency Aviation Cyber Initiative.

**5. Security Governance Division (AIS-100).**

a. Serves as the authority for ensuring effective IT Security governance throughout IS&P. AIS-100 specifies the accountability framework, and ensures that security strategies are aligned with business objectives, adhere to policies and internal controls, and are consistent with applicable laws and regulations; and

b. Oversees the IT Shared Services IS&P Information System Security governance and acts as the managing conduit for interaction with the consumers of the IS&P IT Shared Services.

**(1) Policy, Training & Customer Liaison Branch (AIS-110):**

(a) Develops and updates enterprise cybersecurity and privacy policies in coordination with FAA lines of business and staff offices 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;

(b) Oversees the FAA's annual Security and Privacy Awareness Training, Information Security and Privacy (IS&P) key personnel role based training, and other information security and privacy training as needed. Maintains Key IS&P personnel listing;

(c) Serves as customer liaisons (Information System Security Officers/Privacy Managers) to the Agency's LOBs and SOs and facilitate services, information flow, and remediation activities; and

i. Establishes and supports the AIT Intake processes for IS&P established by BPS which serves as the front door into IT services; and

ii. Acts as a facilitator by connecting customers with appropriate security subject matter experts within IS&P.

(d) Processes cybersecurity, information security and privacy deviations and waivers from IT Security and Privacy policies.

**(2) Security Architecture & Resilience Branch (AIS-120):**

(a) Works with other Security Divisions, Staff Offices and Agency POCs to enable Primary Mission Essential Functions and Essential Supporting Activities continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

(b) Develops and maintains AIT's COOP plans, supports and ensures development of the FAA's Security Architecture;

(c) Ensures that the information security requirements necessary to protect the organizational mission/business functions are adequately documented in all aspects of enterprise architecture including reference models, segment and solution architectures processes; and

(d) Collaborates with the Solution Delivery Service, who is the primary lead for the Enterprise Architect.

**6. Security Compliance Division (AIS-200).** 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, Business Continuity and Disaster Recovery (DR) exercises, Information System Contingency Plan (ISCP) and ISCP testing to include Business Impact Assessments. Additionally, this branch is responsible for Audit and Reporting on data calls from Office of Inspector General and Government Accountability Office, Federal Information Security Management (FISMA), Capital Assessment Project goals, Section M contract reviews and privacy compliance act reviews.

**a. Vulnerability Management Branch (AIS-210):**

(1) Provides services related to monitoring and tracking vulnerabilities within the FAA's FISMA reportable systems. AIS-210 ensures Plan of Action & Milestones (POA&Ms) are entered into the Cyber Security Assessment and Management (CSAM) system. In addition,

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 Memorandum of Agreement/Memorandum of Understanding, coordinates vulnerability scanning, monitors/tracks security incidents, monitoring and tracking binding operational directives and responds to audits related to POA&Ms;

(2) Manages vulnerability mitigation and remediation as identified by the FAA's Data Loss Prevention service, security assessments, vulnerability scans and incident events;

(3) Manages vulnerability mitigation and remediation of all Department of Homeland Security (DHS) Cyber Hygiene scanning vulnerabilities; and

(4) Provides coordination on the scheduling and remediation of vulnerabilities as identified by operating system, web application, database, and dynamic and static code scanning for all FISMA reportable systems in accordance with DOT Cybersecurity Compendium requirements.

**b. Continuity Management Branch (AIS-220):**

(1) Provides business continuity management support to ensure that the agency has an integrated, overlapping COOP capability, so that should disaster strike, the agency can carry out essential functions;

(2) Responsible for all security and privacy aspects of the DR services in coordination with AIT's, APS's, AIF's, ADE's, and AIS's Security Governance division; and

(3) Provides technical SME and advisory support to stakeholders to develop, maintain, and implement the ISCP and DR strategies and solutions, including risk assessments, Business Impact Analysis, strategy selection, and documentation of recovery procedures. AIS-220 supports regular mock-disaster exercises to test existing plans and strategies. Upon activation of the ISCP, AIS-220 provides incident response support by creating and maintaining the incident log, coordinating communications, and providing recovery support and coordination of the incident review activities.

**c. Security Assessment Branch (AIS-230):**

(1) Responsible for scheduling, conducting, and tracking security assessments. AIS-230 reviews completed security assessments and processes for authorization signature. They provide guidance on National Institute of Standards and Technology (NIST) Standards and Publications that relate to the Security Authorization Process and authors the Agency Authorization Handbook;

(2) Develops, reviews, updates PTA, PIA, and System Disposal Assessments (SDA) to ensure systems are appropriately assessed to identify privacy risk, and determine whether additional privacy compliance activities are necessary. Submits PTA/PIA/SDA to the DOT and tracks adjudication status. Provides guidance to System Owners on PTA/PIA/SDA development and resolves any documentation issues. Coordinates with Records Manager and General Council on PTA/PIA and resolves any documentation issues; and

(3) Maintains the Agency's FISMA-reportable IT inventory and required system data in the DOT FISMA Reporting System of Record, CSAM. Provides CSAM account approval and tracking for the Agency.

**d. Audit & Reporting Branch (AIS-240):**

(1) 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. This requires aggregating stakeholder feedback for audits and data calls and then responding to the auditor. AIS-240 provides audit liaison support for external audits with a sensitive awareness of applicable requirements and regulations directed by DOT, OMB, DHS, Office of Personnel Management (OPM), and NIST;

(2) Conducts Section M Contract Reviews, to ensure that FAA contractor systems that handles PII have the appropriate AMS clauses related to privacy incorporated into the contract; and

(3) Conducts regulatory Privacy Compliance Reviews, maintains responsibility for ensuring reporting integrity, makes recommendations on findings, and collaborates with stakeholders in making adjustments to policies, priorities, structure, or procedures to make operations as efficient, economical, and effective as possible.

**7. Security Operations Division (AIS-300).** Responsible for the day-to-day activities to mitigate security and privacy risks at the technical level. The division provides tooling resources and security services, delivers performance metrics, and supports internal and external cyber exercises. The division also hosts the FAA's SOC which provides 24x7 monitoring and technical support to detect security threats and attacks against the FAA.

**a. Cybersecurity Operations Support Branch (AIS-310):**

(1) Provides the authoritative direction, support services, and coordination for security architecture and engineering compliance across the FAA's Mission Support, NAS, and R&D domains. This branch maintains documentation and ensures the tools that are needed to detect adversary attacks are current and available for use by the SOC and partners in the NAS and R&D domains.

**b. Cybersecurity Services Branch (AIS-320):**

(1) Provides tactical execution of cybersecurity services by scanning for and evaluating vulnerabilities and risks. This branch performs vulnerability assessment scan on the operating system, web application, database and application code scans, conducts and facilitates penetration testing, and provides patch management support for systems in all three FAA's domains (Mission Support, NAS, and R&D). Ensures scanning inputs and outputs are complete and concise, shares results with the Vulnerability Management Branch or other requestors, and provides information as needed to respond to data calls; and

(2) Delivers continuous monitoring by providing technical solutions supporting the Agency's CDM program.

**c. Cybersecurity Metrics & Exercises Branch (AIS-330):**

(1) Provides metrics to evaluate the agency's overall cybersecurity performance. They also provide metrics for specific goals related to the detection, disruption, and denial of cyber-attacks, and the detection, response, and remediation of threats and vulnerabilities; and

(2) Executes internal cyber exercises to test the agency's incident response capabilities, and participates in external cyber exercises.

**d. Security Operation Center (SOC) Branch (AIS-340):**

(1) Provides the services needed to detect, analyze, respond to, report on, and ultimately prevent cybersecurity incidents;

(2) Provides incident response, advanced persistent threat analysis, intrusion detection, and forensic analysis services for the FAA Enterprise; and

(3) Consolidates cybersecurity functions by performing the day-to-day activities needed to mitigate IS&P risks at the technical level.

**8. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

# Chapter 9. Chief Data Office (ADO)

**1. Chief Data Office (ADO-1).** Concentrates on the opportunities, threats, capabilities, and gaps related to managing FAA information as a strategic asset and potentially a liability. The office leverages data and information for decision-making, engages industry, manages information for operational efficiency, and manages risk inherent in massive and fast changing data resources through effective governance. The Director has authority to make changes in structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA IT policy and procedures as directed by the CIO. The following is the roles and responsibilities of ADO-1:

a. Has authority to make changes in ADO structure, authority or responsibility to adjust roles and responsibilities to fit its business needs at the directorate level and below, and authority to enforce changes in FAA and Data and Information policy and procedures as directed by the CIO;

b. Provides enterprise data services;

c. Performs enterprise data governance; and

d. Provides enabling functions to facilitate ongoing digital transformation and advances analytics within FAA including business intelligence and reporting services that support decision-making and performance tracking.

**2. Mission:** Enables seamless flow and access of timely, reliable, and relevant information, which supports evidence-based decision-making and innovation for the FAA enterprise and aviation stakeholders.

**3. Data Governance (ADO-010)**. The ADO-010 staff office is responsible for a few key enterprise services.

a. ADO-010 is responsible for facilitating Enterprise Data Governance. This includes:

(1) The Data Governance function guides all other data management functions. The purpose of Data Governance is to ensure that enterprise data is managed properly, according to policies and best practices. While the drive of data management overall is to ensure an organization gets value out of its data, Data Governance focuses on how decisions are made about data and how people and processes are expected to behave in relation to data. The scope and focus of a Data Governance Program includes the following functions:

(a) Strategy: Defining, communicating, and driving execution of the FAA data strategy and data governance strategy;

(b) Policy: Setting and enforcing policies related to data and metadata management, access, usage, and quality (security aspects are currently covered under FAA Cyber Security Orders);

(c) Standards and Quality: Setting and enforcing data quality and data architecture standards;

(d) Oversight: Providing hands-on observation, audit, and correction in key areas of quality, policy, and data stewardship;

(e) Compliance: Ensuring the agency can meet data-related regulatory compliance requirements;

(f) Issue Management: Identifying, defining, escalating, and resolving issues related to data security, data access, data quality, regulatory compliance, data stewardship, policy, standards, terminology, or data governance procedures;

(g) Data Management Projects: Sponsoring and facilitating efforts to improve the agency's data management practices; and

(h) Data Asset Valuation: Setting standards and processes to consistently define the mission/business value of data assets.

b. ADO-010 is responsible for coordinating external access to data. This includes management of data.faa.gov and api.faa.gov; and

c. ADO-010 is responsible for facilitating FAA's compliance with Open Government Data Act, Geospatial Data Act and related guidance from OMB.

**4. Data Services and Platforms (ADO-020)**. The ADO-020 is responsible for several AIT provided enterprise data services and platforms:

a. The ADO-020 staff office will be responsible for the design, development, and sustainment of AIT managed data platforms, data warehouses, API infrastructure and external data access portals. These capabilities will be delivered with a product focus. The ADO-020 is responsible for:

(1) Establishes and maintains relationships with the key business and technology stakeholders who guide decisions regarding product capabilities and priorities;

(2) Performs (internal or external) customer research by means of including surveys, product analytics, market research, interviews, hackathons, online forums, or other cost-effective means of gaining insight into the "voice of the customer." Use this insight to define the customer segments the product will target, to understand those customers' goals, and how they would gain value from product capabilities;

(3) Performs competitive analysis on the alternatives that target customers might use, so as to understand what capabilities and qualities the enterprise capabilities must incorporate;

(4) Facilitates and drives alignment among key stakeholders, supplying customer and market research and analytics to lead them to converge on a product strategy, vision and roadmap;

(5) Works within the product budget established in consultation with business sponsors and AIT management by balancing resources across customer and market research, competitive analysis, vision development, and prototyping, but primarily to sustain product teams to deliver and maintain the service or platform;

(6) Works with key stakeholders to make frequent and dynamic prioritization decisions based on the latest product analytics, product team metrics and customer feedback. Define, track and communicate key product performance indicators as required to inform this process, and track business results;

(7) Works with key stakeholders to develop and refine business and cost models for the product;

(8) Ensures that the organization is prepared to deliver and support the entire business capability (including all of its human, organizational, process and physical aspects, such as training for help desk and support teams); and

(9) Continually monitor and refine the product.

b. Acts as the "keeper (and communicator) of the vision" to translate the product strategy and vision developed with business stakeholders into what the product team must bear in mind every day to ensure they are building the right product. This includes:

(1) Defines the product roadmap based on business outcomes;

(2) Collaborates closely with product delivery teams and with other product managers within the product line, to avoid duplication and manage dependencies;

(3) Coordinates with other stakeholders such as business, data and IT architects to align product and platform architectures and capabilities according to agreed goals for nonfunctional requirements; and

(4) Collaborates and coordinates with innovation teams to manage the flow of new ideas and product capabilities into one or more product lines. Product managers should be aware of innovation efforts and actively encourage an ecosystem of innovators around their product domain, possibly including external ecosystem developers and partners.

**5. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

## Chapter 10. Administration

**1. Organizational Chart.** The organization chart is available on the MyFAA employee website: https://my.faa.gov/content/dam/myfaa/org/staffoffices/afn/information/AIT-Organization- Chart.pdf.

**2. Distribution.** This order is distributed to the division level in Washington headquarters, regions and centers with distribution to each field office and facility.

## Appendix A. Form

U.S. Department of
Transportation
**Federal Aviation**
**Administration**

### Appendix A. FAA Form 1320-19, Directive Feedback Information

Please submit any written comment or recommendation for improving this directive, or suggest new items or subjects to be added to it. Also, if you find an error, please tell us about it.

Subject: FAA Order IT 1100.XX – Office of Information and Technology (AIT) Organization (OPR: ASP-110)

To: Directives Management Officer, ASP-1

*(Please mark all appropriate line items.)*

☐ An error (procedural or typographical) has been noted in paragraph on page

☐ Recommend paragraph on page be changed as follows:
*(Attach separate sheet if necessary.)*

☐ In a future change to this Order, please cover the following subject:
*(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____
FAA Form 1320-19 (10-98)