U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Information and Technology National Policy

ORDER
IT 1100.171B

Effective date:
01/28/24

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, governance and has primary FAA oversight responsibility for all Agency IT investments. The CIO promotes and guides FAA IT direction that supports the FAA Strategic Goals of Safety, People, Global Leadership, and Operational 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-001)
- Strategy & Performance Service (ASP-001)
- Enterprise Program Management Service (AEM-001)
- Business Partnership Service (APS-001)
- Solution Delivery Service (ADE-001)
- Infrastructure & Operations Service (AIF-001)
- Information Security & Privacy Service (AIS-001)
- Chief Data Office (ADO-001)

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

NATESH M MANIKOTH Digitally signed by NATESH M MANIKOTH
Date: 2024.01.28 13:25:26 -05'00'

Natesh Manikoth
Acting Deputy Assistant Administrator
for Information & Technology and CIO, AIT-1

Table of Contents

Table of Contents

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; Orders and Notices and on the public website; Orders and Notices.

4. What This Order Cancels. This Order cancels IT 1100.171A, Office of Information and Technology (AIT) Organization, dated 08/01/2020.

5. Reference. Department of Transportation (DOT) Order 1351.39 IT Management Policy or current version; CIOP Chapter 1351.39 Departmental Information Technology Governance Policy.

6. 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-001/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 IT 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, People, Global Leadership, and Operational Excellence 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 (IT 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, if required.

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 and AMS Procurement Policy & Guidance.

g. Serves as the Chairperson, IT Shared Services Committee (ITSSC). The chair receives facilitation and management support from the ITSSC Secretariat. The chair will appoint the AIT-2 to chair the meeting if AIT-1 is unable to chair the meeting. The purpose of the ITSSC is to enable IT service providers and business partners across the FAA to discuss enterprise-wide technology matters. This is an informal forum to share IT initiatives and updates that may impact agency operations and require executive-level- buy-in or collaboration.

h. The CIO considers guidelines as outlined in DOT Order 1351.39 IT Governance Policy, Section 39.5, or current version.

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 & 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-001).

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 Strategy & Performance (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 enterprise level policies, and provides program management and compliance oversight for the FAA Directives, FAA Forms, FAA Records Management, FAA Paperwork Reduction Act, and FAA Section 508;

(2) Coordinates and maintains IT-related policies and provides program management and oversight for Orders and the National Archives and Records Administration;

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

(4) 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 Software Asset Management services in the administration of enterprise software policies and procedures. Manages the optimization of compliance, contracting, procurement, deployment, maintenance, utilization and disposal of software in the FAA environment. The division contributes to strategic and business planning and analysis activities, and serves as a liaison between FAA and the IT industry. Explores, evaluates, and conducts proactive strategic research and analysis of emerging and innovative technologies.

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

(1) Performs Vendor Management activities in selection, cost control, and contract and risk management to ensure optimal software service delivery for the FAA;

(2) Works with the FAA Acquisition & Contracting Office and vendors to negotiate the best price and value position for the FAA on software acquisitions;

(3) Manages and serves as vendor lead and COR for FAA's enterprise software licensing/subscription contracts and agreements;

(4) Tracks license/subscription utilization and conducts internal reviews of installed software products and collaborates with vendors to ensure compliance with FAA contracts, agreements and license terms and conditions;

(5) Maintains the FAA software inventory baseline and implements software harvesting and license reclamation processes;

(6) Concentrates on software lifecycle governance and Software as a Service utilization; and

(7) Processes all requests for software to be installed on FAA IT assets according to technical standards, license terms and conditions, and security and compliance criteria.

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

(1) Develops agency-wide Software Management policy and processes;

(2) Develops and implements metrics and metrics methodologies supporting tracking of software request fulfillment time-to-deliver, identification of workflow gaps, and cultivation of strategies for continuous service improvement;

(3) Facilitates the FAA Enterprise Software Board responsible for adjudication of requests for software with a limited scope, contained lifecycle or not listed on the Technology Product List/Technology Product Roadmap (TPL/TPR);

(4) Facilitates the FAA CIO Package review/approval process. 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) Coordinates responses for software management reporting, and exchange of information with DOT and other Federal agencies to comply with the Federal Information Technology Acquisition Reform Act and other government laws and guidance/memoranda;

(6) Manages the FAA enterprise software license inventory and software purchase records database;

(7) Manages initiatives focused on software license currency, reducing security risk posed by software, including but not limited to Enterprise Operation-critical software, software rationalization and unauthorized software;

(8) Provides Software COR support for the FAA Strategic Sourcing for the Acquisition of Various Equipment and Supplies (SAVES) contract; and

(9) Serves as the AIT Mobility Service Coordinator in the provisioning of mobile devices for the AIT workforce.

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, 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.

b. IT Commodities Purchasing Section (ASP-311):

(1) Processes PC transactions utilizing the FAA's PRISM ensuring that the goods or services requested are received in a timely manner;

(2) Reconciles PC transaction with the FAA's bank vendor to ensure accuracy and makes corrections as needed; and

(3) Reconciles IT shipping transactions with vendor invoices and makes corrections as needed.

c. Hardware Asset Management Branch (ASP-320):

(1) Concentrates on Life Cycle Management (LCM) for FAA printers;

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

(3) Develops and maintains policies, standards, processes, systems, and measurements to manage the FAA enterprise print environment; and

(4) Performs AIT Property Delegate duties, including assistance with lost equipment.

d. Life Cycle Management Branch (ASP-330):

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

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

(3) Manages the addition to the property system of record, transfers the assets to/from the LOBs/SOs and performs the disposal of IT equipment that is no longer required by the agency.

6. Contract Strategy & 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, IAAs, FAA SAVES hardware contracts, and serves as the Program Office for the Supply Order Tracking program and printer consumable requests/purchases and order tracking. This division provides coordination and approvals on applicable CIO requests and approval. 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;

(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; and

(6) 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.

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: AIT Organizational Chart.

Chapter 4. Enterprise Program Management Service (AEM)

1. Director of Enterprise Program Management Service (AEM-001).

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) Project Manager (PM) is deployed when all Project Management Life Cycle (PMLC) documentation is required to support an IT Development Project that does not have a PM leading it (Federal (FED) or Vendor Contract (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) IT Project Manager (IT PM) is deployed when all PMLC documentation is required to support an IT Development Project that has a PM leading it (FED or Vendor CTR) from a non-AIT LOB/SO. 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; and

(c) 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 program 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 objectives; 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; and

(2) [Reserved]

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, Office of Audit and Evaluation, AHR and AIT projects; and

(2) Business Management Portfolio B Branch (AEM-320): Supports AFN, 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; and

(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 in managing all aspects of the portfolio;

(c) Manages EPMS's Integrated Master Schedule; and

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

7. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

Chapter 5. Business Partnership Service (APS)

1. Director of Business Partnership Service (APS-001).

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

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

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

2. Intake & Portfolio Management Staff Office (APS-010). This Team is the front door for all external stakeholder requests. They are:

a. Responsible for tracking stakeholder requests coming into AIT and routing requests appropriately for rapid fulfillment;

b. Provides executive level metrics and dashboards to AIT leadership on incoming requests from stakeholders;

c. Responsible for coordinating internal AIT requests for resources from other AIT service areas via the Enterprise Resource Request process, which tracks requests for resources and fulfillment of resources from one AIT service area to another;

d. Responsible for coordinating and facilitating periodic reviews with stakeholders. Works collaboratively with the AIT verticals to develop executive level briefings for stakeholder organizations focused on their current IT activities, portfolio management and critical issues. Portfolio reviews are used to highlight upcoming AIT initiatives, and address questions and concerns from the stakeholder LOB or SO;

e. Responsible for gathering and reporting Core Services metrics for all AIT services at the executive level, reporting on Core Services trends, incidents and anomalies. Responsible for managing reports, dashboards, and metrics relating to AIT Core Services Metric process; and

f. Responsible for overseeing the External Funding Agreement (EFA) request process. An EPA is required for most AIT services or solutions that are funded by FAA Business Partners. The EFA Coordinator facilities the completion of all EFA requests and provides general support to all EFA stakeholders, including data management, dashboard management, and reporting.

4. Experience Management Office (XMO) (APS-020). The Experience Management Office (XMO)'s goal is to enable the FAA mission by ensuring the FAA workforce can execute what they do flawlessly through the use of technology. To do this, the XMO:

a. Performs holistic experience engagements, using human centered design methodology, that identify and reduce friction points for AIT's end users;

b. Produces experience reports that hold AIT accountable for designing and delivering services with a focus on the experience of people interacting with our products and services;

c. Provides the tools, knowledge, and training the AIT workforce needs to enhance the total experience of FAA IT; and

d. Operates and maintains the AIT Experience Center, "The Runway," which provides a physical and virtual space for FAA to interact with technology in an accessible and approachable way, helps AIT understand how FAA uses or might use technology to advance the mission, and provides an opportunity for FAA to experience emerging technologies that can enhance their work experience.

5. 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.

6. Customer Support Services Division (APS-200). Manages the MyIT Service Catalog and all activities.

a. Service Catalog Branch (APS-210):

(1) Manages the MyIT Service Catalog, 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; Ensures that the IT workforce is knowledgeable about IT capabilities and services that are available to the business; and

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

b. User Education and IT Advocacy Branch (APS-220):

(1) Provides solutions that improves the user's knowledge and understanding of 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 user's knowledge and understanding;

(3) Coordinates the development of training material as needed to enhance the overall knowledge and understanding of FAA users; and

(4) Provides guidance and content to the stakeholder outreach initiatives, such as the Training & Educational Lunch and Learn series, to provide information to improve the overall knowledge and understanding of the products and services provided by AIT.

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

a. Service Management Branch (APS-310):

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

(2) Oversees Process Improvement activities (i.ie., creation of Knowledge Based Articles in conjunction with contract staff including coordination with other AIT and BPS groups for process improvement changes;

(3) Reviews and provides oversight on Service Center contract including evaluating monthly performance metrics and determining contract compliance;

(4) Facilitates and improves service delivery activities for Service Desk; and

(5) Performs Service Measurement activities reviewing incident/project ticket trend analysis and feeds outcomes of analysis into improvements including process update or system enhancements.

(a) Helpdesk Operations Section (APS-311):

i. Provides management and oversight of the ATO Tech Ops Maintenance Data Terminals (MDTs), and supports the coordination for hardware activities related to MDT's including facilitation of assistance from other AIT groups, local FAA facility activities, and MDT special projects which require support from the Service Operation Branch;

ii. Assists Service Management with oversight on the Service Center contract including evaluating monthly performance metrics and determining contract compliance; and

iii. 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, offsite events (Sun-n-fun, Oshkosh, etc.), and associated project related activities.

(b) [Reserved]

b. Service Operations Branch (APS-320):

(1) Service Desk Tier 1-2 Operations:

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

(b) Directs support staff to follow IT 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;

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

(d) Identifies, streamlines, and implements IT processes to improve overall stakeholder experience.

(2) Incident Management:

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

(b) Provides briefings to PBS and AIT management on escalation tickets, trends, and status updates to resolve mission critical tickets and urgent escalations making recommendations to improve overall customer support services.

(3) Event (VIP) Management:

(a) Oversees VIP/Executive support for AIT tickets and projects along with the self-service tools available. Provides reporting of all VIP/Executive incident/request related data sets including Service Desk calls, incidents, requests, outages, projects and trend analysis;

(b) Provides contract oversight for VIP Support contractors and completes daily reports outlining contractor activities in relation to VIP/Executive tickets; and

(c) Provides daily briefings to BPS management on VIP/Executive tickets, escalations, trends, and status updates to resolve tickets timely. Works closely with other AIT and FAA Front Office management on VIP/Executive Support activities.

8. 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, IT 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.

9. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

Chapter 6. Solution Delivery Service (ADE)

1. Director of Solution Delivery Service (ADE-001).

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 business partners; and

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

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 "back office" to Solution Delivery (SD):

a. Tracks and monitors work assigned, manages the demand for resources and the total cost to the taxpayer model for supported applications;

b. Manages the business of ADE including budget, financial and business planning, training strategy, and the SD Landing Page;

c. Visibilities into ADE activities and projects and understands the pipeline of inbound work;

d. Oversees the Solutions Work Assignment Team, ensuring the efficient intake of work;

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

f. Ensures ADE processes are documented, maintained, and accessible to employees; and

g. Serves as a liaison between the process authors within ADE's Divisions and ASP for process development, coordination, and related activities.

3. Quality Management Division (ADE-100). Ensures products are suitable for their intended purpose, meet requirements, and operate to business partner expectations.

a. Quality Assurance Branch (ADE-110):

(1) Provides Quality standards guidance and quality audits; tracks compliance and reports; oversees lessons learned and process improvement; and

(2) Holds Quality Forums regularly; and ensures accessibility and Section 508 compliance, as required.

b. Quality Operations Branch (ADE-120):

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

(2) Works 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;

(3) Elicits, documents and maintains product requirements;

(4) Provides Quality Assurance and Test Management support by ensuring the identified software development methodology is followed, standards are met and the product is suitable for its intended purpose and works correctly; and

(5) Overseeing the products test execution, including functional, regression, user acceptance interface/system, compatibility, and performance/load and accessibility testing.

c. Citizen Development Facilitation Office Branch (ADE-130):

(1) Facilitates Intelligent Automation (IA) for the FAA. This includes evaluation and section of IA technologies, establishing the governance for these technologies, ensuring they are secured and accessible for traditional Citizen Development or leveraging a 3rd party integrator. These technologies consist of Robotic Process Automation (RPA), Business Process Automation (BPA) and Low Code Application Platforms (LCAP);

(2) Solution Shepherds assist business partners navigating the Solution Factory with high-level requirements, SOWs, SSJs; solution options, solution selection, implementation and cross-functional collaboration or coordination as required; and

(3) Community outreach and socialization of our services consisting of Lunch & Learns, office hours, Communities of Practice (CoP), access to product training, playbooks, and technology challenges.

4. Enterprise Architecture and Portfolio Insight Division (ADE-200). Serves as the FAA Mission Support Chief Architect to align technology products and business partner portfolio applications to the goals, processes, and security standards within AIT and the FAA.

a. Enterprise Architecture Branch (ADE-210):

(1) Provides Investment Support and Governance services: conducts Enterprise Architecture reviews on Facility and Equipment (F&E) investments; develops the annual Enterprise Architecture Roadmap for F&E investment decision points; manages Architecture Change Notices; and serves as the secretariat of the Architecture Review Board and the FAA Enterprise Architecture Board;

(2) Provides Segment and Domain Architecture (SDA) services: maintains the Solution Factory Security Architecture Framework; conducts the annual DOT Maturity Assessments; serves as the Enterprise Architecture member of the Acquisition Readiness Team; develops AIT enterprise level service roadmaps; and maintains the Business Process Model reference model; and

(3) Provides Enterprise Architecture Management System (EAMS) services: serves as the system owner for EAMS; facilitates EAMS as the authoritative inventory and data source for enterprise wide technologies and software solutions; processes enhancements to EAMS based on customer requests; and manages integration between EAMS and other data sources.

b. Technology Standards Section (ADE-211):

(1) Serves as the chair for the Technology Control Board meetings to review, assess, and approve IT products, services, and standards used in the FAA;

(2) Develops technology standards, in accordance with information system security standards to ensure consistency; and

(3) Maintains the FAA's TPL which constitutes the authoritative source of sanctioned technology products (hardware, software, network and storage) for use throughout the Agency.

(4) Provides investment decisions support.

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

(1) Provides product portfolio management of FAA software solutions by maintaining a "living' product roadmap;

(2) Collaborates with AIT Project Managers, DevOps Leads, Sustainment Leads, BPMs, Enterprise Architects, Security Specialists and others to have the latest information on current and future improvements for the TPR;

(3) Captures solution related information such as security, finance, technology, or business related impacts;

(4) Promotes technology solution alignment to business goals, use of common technology platform(s), and achievement of enterprise-level security and scale;

(5) Functions as Solution Brokerage; assembling reference solutions, maintaining the Solution Cache, assisting business partners with gathering their requirements, RFIs, and facilitating solution development; and

(6) Works closely with the Citizen Development Facilitation Office (CDFO, ADE-130), Solution Development (ADE-510) and Enterprise Architecture (ADE-210) teams to record future plans for FAA solutions.

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; and

(2) Responsible for the Knowledge Services Network (KSN) enterprise service, enterprise collaboration projects, operational support for the SharePoint Online, Lists, and OneDrive components in the Microsoft 65 environment.

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

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

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) Provides system administration and application deployment services for staging and production servers hosting application and web platforms for custom built applications; and

(4) Automates deployments using DevSecOps methodologies, streamlining AIT's deployment of applications.

b. Database Management Branch (ADE-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. Development and Sustainment Division (ADE-500). Responsible for development and operations of custom applications, including application security and system security compliance support. ADE-500 is also leading the effort to modernize and secure these custom applications (e.g., minimal technical debt) for the enterprise using modern architecture patterns and methodologies like DevSecOps, Agile Development, Test Driven Development (TDD) and others.

a. Solution Development Branch (ADE-510):

(1) Responsible for the logical and physical design of custom applications which include business applications, web applications, service-driven applications and others;

(2) Oversees and manages the conceptualization, detailed design, and development of custom applications that attempt to maximize the reuse of secure FAA IT enterprise services and adhere to FAA enterprise technology and security standards;

(3) Provides product management support, including oversight over greenfield and brownfield development efforts; and

(4) Ensures that delivered solutions are of consistently high quality, are delivered against a clear and stable set of functional and non-functional requirements, promote an application architecture that aligns with standards and promotes loose coupling and standards-based architecture, and are operationally fit.

b. Solution Operations A Branch (ADE-520): Provides product management and technical support for applications that are in sustainment mode. The product support managers' responsibilities are described (Section 6, Paragraph 7d.(1) – (4)).

c. Solution Operations B Branch (ADE-530): Provides product management and technical support for applications that are in sustainment mode. The product support managers' responsibilities are described (Section 6, Paragraph 7d.(1) – (4)).

d. Solution Operations C Branch (ADE-540): Provides product management and technical support for applications that are in sustainment mode. The product support managers' responsibilities are described (Section 6, Paragraph 7d.(1) – (4)). Their responsibilities are described below.

(1) Manages business applications in AIT's application portfolio;

(2) Provides application product management support by overseeing the operations, break/fix, maintenance, environment upgrades, minor requests from AIT's business partners, and

(3) Works closely with internal and external application stakeholders to ensure the application's overall health by ensuring the application is available, technically viable, secure, and has appropriate up to date documentation, and

(4) Provides Tier 3 support to applications.

e. System Security Compliance Branch (ADE-550). Provides insight into the ADE portfolio of solutions and products, particularly the solutions' posture in terms of cybersecurity vulnerabilities. Leverages technologies like data analytics, RPA, and others, to provide strategic information to ADE.

(1) Compliance Support & Vulnerability Reporting Section (ADE-551):

(a) Provides security expertise to all ADE products, systems and solutions and engages the various stakeholders within AIT;

(b) Provides IT security advisory services to the ADE organization;

(c) Provides IT System Ownership services for ADE-500 managed applications and systems;

(d) Provides guidance to establish the system Federal Information Security Modernization Act (FISMA) information types and accreditation requirements, including continuous monitoring for the duration of the system development life cycle;

(e) Provides operational security recommendations, improvements, best practices, standardized configuration baselines, hardware/software solutions, and monitoring strategies to safeguard data efficiently;

(f) Tracks and monitors risks, threats, vulnerabilities, and remediation solutions to adequately analyze and interpret the risk impact on system boundaries; and

(g) Determines system control inheritance and common control strategy improvements.

(2) [Reserved]

8. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

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 Network 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, including Trusted Internet Connections, IT data centers, including cloud and end point client devices.

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. Enterprise Operations Center (AIF-010). The Enterprise Operations Center's (EOC) mission is to provide automated 24x7 monitoring, alerting, performance, reliability and optimization services for systems and infrastructure in the FAA. The EOC uses predictive analysis methods to anticipate issues before they occur, reduce service interruptions, and maximize service uptime. The EOC also provides live monitoring, AIF Communications and troubleshooting for critical IT Systems and Services through continuous monitoring, AIF identifies interruptions to systems and service as soon as they occur.

a. 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

b. 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.

3. Business Management Services Division (AIF-100). Serves as the front door to the AIF organization and provides enterprise reporting, performance and resource management for all AIF workloads and projects. Responsible for AIF SOPs and business processes, including change and configuration management, to promote effective and efficient operations as well as protect operational environments from harm.

a. Enterprise Reporting and Metrics Branch (AIF-110):

(1) Establishes, monitors, and reports on overall metrics and performance targets for AIF and AIT. 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

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

b. Resource Management Branch (AIF-120):

(1) 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;

(2) Manages AIF's work intake. 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. Provides input into the portfolio planning process and coordinates inputs into Service Level Agreements;

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

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

c. Business Process Management Branch (AIF-130):

(1) Responsible for AIF SOPs and business processes, including managing AIT's Enterprise Change and Configuration Management Process, focusing on the efficient, effective, and comprehensive management of all changes to the IT production environment;

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

(3) Utilizes standardized methods and procedures to efficiently categorize, authorize, and schedule requests for changes to the IT production environment to minimize the number and impact of related incidents on service. Responsible for receiving, logging, prioritizing, and facilitating the completion of all change requests. This includes updates to the change log with all progress as it occurs, closes requests for completed changes, and provides reports to management on all known changes to the IT production environment;

(4) 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

(5) As the Librarian of all Configuration Items (CIs), works closely with Asset Management, Cybersecurity, and Service Catalog teams to ensure AIT has a clear picture of all CIs and CI-related assets within the Configuration Management Database (CMDB). Configuration Management processes will include identified attributes to ensure the CMDB accurately reflects the relationships and dependencies of the CIs. Manages the CMDB.

4. Service Delivery Division (AIF-200). Provides comprehensive management and oversight of AIT's test and production environments. Manages the transition process from test to production and is responsible for the planning, scheduling, bundling, releasing of all deployments. Additionally, Focuses on continuous delivery through innovation and automation, leveraging new technologies to rapidly deliver quality I&O services.

a. Continuous Delivery Branch (AIF-210). Collaborates within AIF and across the AIT Services to research, develop, and implement automated ways to improve continuous service delivery and streamline business processes.

b. Deployment Management Branch (AIF-220):

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

(2) Ensures that releases are clearly defined and successfully transitioned into production. 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, 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. 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 Endpoint Services and AIF's Device Management Branches, to ensure operability and successful deployments and installations on endpoints.

c. Pre-Production, Test & Evaluation 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.

5. 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 authentication and directory services, account and access management, network operations and infrastructure services.

a. Authentication 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) 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

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

b. Network Management Branch (AIF-320):

(1) Enables the successful operation of the FAA's network systems and services including LANs, WANs and integrations with FAA Cloud Services (FCS), Colocation facilities, and FAA Telecommunications Infrastructure (FTI). Administers, configures, manages, and troubleshoots the infrastructure that protects the FAA's network, including switches, routers, and wireless; and

(2) Maintains availability of network services. Provides network guidance to facilities that are new, moving, or renovating and coordinates the installation of new network circuits. Plans, designs, and modernizes network topologies and configurations and sets standards for network technologies.

c. Infrastructure Services Branch (AIF-330):

(1) Enables the successful operation of the FAA's network systems and infrastructure services including Trusted Internet Connections (TICs), DDI, Network Access Control (NAC), and firewalls. Administers, configures, manages, and troubleshoots the infrastructure that protect the FAA's network, including firewalls, NAC, Bluecoat, Infoblox, and IronPort; and

(2) Maintains availability of network services and works closely with the Network Branch to schedule and implement updates to all network services. Detects, diagnoses, troubleshoots, and resolves all network services outages and performance issues as they are identified.

d. Account & Access Management Branch (AIF-340):

(1) Authenticates and organizes user accounts and services on the FAA network;

(2) 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

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

6. Cloud & Hosting Services Division (AIF-400). Responsible for the management of the hosting environments, cloud, co-location and on-premise. Provides full scope of hosting management, including contract management, stakeholder management, architecture and engineering, governance through Center of Excellence and operations and maintenance of all hosting environments.

a. Hosting Management Branch (AIF-410). Provides a full scope of product management support, including contract management, CCOE, stakeholder management, and architecture and engineering across all hosting environments (cloud, co-lo, and on-premise). Assesses the provisioning of hosting solutions for AIT's stakeholders at FAA's data centers, Co-location facilities, and FCS providers.

b. Operations and Maintenance Branch (AIF-420):

(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. Supports hosting file share resources for FAA field shares; and

(2) Executes the provisioning of hosting solutions for AIT's stakeholders at FAA's data centers, Colocation facilities, and FCS providers. Supports hosting file share resources for FAA field facilities. Responsible for securing and managing AIT's operating systems, servers, virtual infrastructure, storage and backup solutions, and the F5 application load balancer servers. 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, both on premises and in FCS.

7. Product & Service Management Division (AIF-500). Responsible for ensuring managed products and services are continually developed so stakeholders can take full advantage of these managed offerings. Supports managed products and service delivery, ensuring operational and digital services deliver positive end-to-end customer experience and operational efficiency with focus on continuous delivery of products.

a. 365 Productivity Branch (AIF-510):

(1) Responsible for the system administration and operation of the FAA's Microsoft Office cloud messaging service;

(2) Supports accounts that provide email, instant messaging, and e-archiving services;

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

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

b. Endpoint Services Branch (AIF-520):

(1) Responsible for management and support of all end points, including image, health, patching, anti-virus and encryption. Ensures all endpoints (laptops, workstations, iOS devices, tablets) are managed securely and consistently;

(2) Responsible for patching clients, 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-521, manages, configures and sets standards for Mobile Devices including, but not limited to, iOS version, iTunes version, and configuration of Mobile Devices; and

(3) 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. Architects hardware and software required to operate the FAA client.

(a) Device Management Section (AIF-521):

i. Responsible for the system administration, product management and operation of the Mobile Device Management system, which currently enables secure access to FAA network resources for approximately 15,000 government-furnished mobile devices, with capability of managing all endpoint device;

ii. Also includes management of group policy, including development and implementation; and

iii. Responsible for the system administration and operation of the agency's anti-virus and full disk encryption, which provides protection to FAA's non-NAS network systems. Implements configuration settings to ensure the security and protection of these systems.

(b) [Reserved]

8. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

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: Policy;

(2) Performs the operational day-to-day activities intended to mitigate information security and privacy risks at the technical level;
Develops and delivers IT security policy, architecture, standards, best practices, and privacy management for the FAA; and

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

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) Oversees the development and maintenance of FAA's Information Security and Privacy Policy and supplemental implementing directives. Ensures collaboration with FAA LOBs and SOs. Signs and authorizes the supplemental implementing directives for FAA Order 1370.121 after concurrence from CSC and the CIO;

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

(4) Serves as the chair of the Cybersecurity Steering Committee (CSC). The CSC is the Risk Executive for the FAA; and

(5) 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;

b. Implements accountability and continuous improvement of FAA privacy processes and programs;

c. Reviews and approves privacy compliance documentation, including Privacy Threshold Assessment (PTAs), Privacy Continuous Monitoring (PCM), Privacy Impact Assessment (PIA) and System Disposal Assessment (SDA) to ensure systems are appropriately assessed to identify privacy risk, and determine whether additional privacy compliance activities are necessary;

d. Tracks and submits document to DOT Chief Privacy Officer for adjudication;

e. Provides guidance to System Owners on privacy documentation development and resolves any issues;

f. Coordinates with Records Management and General Council to resolve any issues;

g. Manages the System of Record Notice (SORN) process. Provides guidance to program offices when drafting new notices and provides updates to old notices;

h. Manages the Identity Monitoring Code issuance process, responds to FAA privacy incidents, and oversees the handling of privacy requests, appeals, and complaints;

i. Supports teams within IS&P who are performing privacy risk assessments, privacy awareness training, writing policy, privacy audits and privacy audit tracking;

j. Responsible for review and update of Social Security Number (SSN) Reduction Plan;

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

l. Responds to Privacy Incidents and works closely with the SOC on information security incidents involving privacy data; works closely with AOC during privacy incidents that generate media interest.

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

a. Manages the security dashboard and reporting mechanisms that support communication of the current state of security and privacy of the enterprise. These dashboards provide a window into security posture of agency computers, servers and other devices on the network. Splunk is a data visualization tool that produces customized reports. Alerting IT managers to the most critical cybersecurity risks. In addition, develops dashboards and reporting mechanisms using Splunk to send data to the CDM agency dashboard at DOT;

b. Manages the data loss prevention (DLP) program. Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or other personal identifiable information (PII) such as social security numbers. To help protect this sensitive data and reduce risk, we need a way to prevent our users from inappropriately or inadvertently sharing sensitive information with people who shouldn't have it. This practice is called DLP. DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed for primary data matches to keywords, by the evaluation of regular expressions, by internal function validation, and by secondary data matches that are in proximity to the primary data match. Beyond that DLP also uses machine learning algorithms and other methods to detect content that matches defined DLP policies;

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;

d. Provides technical SME and advisory support to stakeholders related to Cloud Service Providers (CSP) and Federal Risk and Authorization Management Progress (FedRAMP); and

e. Assists with developing the FAA wide Supply Chain Risk Management (SCRM) strategy and plan. Participates with other LOBs and SOs on FAA wide implementation of SCRM.

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

a. Provides security to the enterprise by strengthening the security of the Aviation Ecosystem through 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 risk identification and activities and information exchange;

(1) Serves as Tri-Chair for the interagency Aviation Cyber Initiative (ACI);

(2) Oversees various ACI initiatives, especially in the areas of training, research and development initiatives, and community exchanges;

(3) Develops collaborations with Aircraft, A-ISAC, and Airlines and Airlift Stakeholders for long-term engagement;

(4) Develops collaborations with Airports Stakeholders for long-term engagement;

(5) Develops internal collaborations with Aviation Safety, Security, NextGen (esp. FAA Technical Center) and Air Traffic Organization cybersecurity stakeholders for long-term engagement;

(6) Establishes relationships with Aviation Management Stakeholders for long-term engagement; and

(7) Establishes relationships with International Stakeholders (esp. International Civil Aviation Organization) for long-term engagement.

b. Identifies aviation ecosystem cybersecurity risks and collaborates with stakeholders to provide opportunities for risk reduction and enable improved resiliency. Enables a cyber-secure and resilient aviation ecosystem as a trusted partner within FAA for strategic cybersecurity stakeholder engagement. Engages in information sharing in support of aviation ecosystem cybersecurity improvement by participating in discussions, forums, conferences, etc; and

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. Works closely with partners, both government and industry, to improve and leverage information, communications, preparation, and defense actions needed to protect FAA systems and networks. Engages in and expands information sharing, guidance, best practices, and collaborations to improve the cybersecurity of the Aviation Ecosystem. Identifies, assesses and analyzes cyber threats, vulnerabilities, and consequences within the Aviation Ecosystem through support of research, development, testing, and evaluation initiatives, engages with Aviation Ecosystem stakeholders on activities for reducing cyber risks, and seeks potential improvement opportunities and risk mitigation strategies:

(1) Rulemaking and standards development support;

(2) R&D Support;

(3) Support for the interagency ACI; and

(4) Cybersecurity Training.

d. Advances global aviation safety, operational excellence and innovation by leading and collaborating with aviation authorities globally.

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;

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; and

c. Coordinates significant activities reporting for all AIS divisions and SOs to AIS leadership for reporting to senior FAA leadership.

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

(a) Develops and updates enterprise cybersecurity and privacy policies in coordination with FAA LOBs and SOs 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;

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

iii. Coordinates with and guides systems owners and other relevant personnel with developing/updating required security assessment documents in preparation for the annual security assessment.

(d) Processes and tracks information security and privacy deviations requests (waivers) from IT Security and Privacy policies risk acceptance memos, and production data usage requests. Coordinates with the requester to complete relevant information for the request. Identifies the risk to the FAA. Coordinates appropriate signatures for each request; briefs AIS leadership on each requests and the risk to the FAA, and submits the request to the FAA CISO and CIO for signature.

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

(a) Works with other Security Divisions, SOs 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, monitors/tracks security incidents, Business Continuity and Incident Response Plans (IRPs) 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), 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;

(2) Ensures Plan of Action & Milestones (POA&Ms) are entered into the Cyber Security Assessment and Management (CSAM) system;

(3) 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, monitors/tracks security incidents, monitoring and tracking binding operational directives (BODs), emergency directives (EDs) and responds to audits related to POA&Ms;

(4) Manages vulnerability mitigation and remediation as identified by the FAA's Data Loss Prevention service, security assessments, vulnerability scans and incident events; Manages vulnerability mitigation and remediation of all Department of Homeland Security (DHS) Cyber Hygiene scanning vulnerabilities and enters tickets in Cybersecurity Incident Management System (CSIMS);

(5) Tracks and manages vulnerability mitigation and remediation of all Cybersecurity and Infrastructure Security Agency (CISA) identified vulnerabilities; and

(6) Provides coordination and technical SME advisory support to System Owners and/or their support staff to develop, maintain and implement the 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 continuity management services to stakeholders in coordination with AIT's, APS's, AIF's, ADE's, and AIS's Security Governance division;

(3) Provides technical SME and advisory support to stakeholders to develop, maintain, and implement the ISCP and incident response plans (IRPs) strategies and solutions, including risk assessments, Business Impact Analysis, strategy selection, and documentation of recovery procedures;

(4) Supports regular mock-disaster exercises to test existing plans and strategies. Upon activation of the ISCP;

(5) Provides incident response support by creating and maintaining the incident log, coordinating communications, and providing recovery support and coordination of the incident review activities; and

(6) Provides technical SME and advisory support to stakeholders to develop, maintain and implement the IRPs.

c. Security Assessment Branch (AIS-230):

(1) Responsible for AIT FISMA reportable inventory scheduling, conducting, and tracking security controls assessments. 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) Reviews and submits SDA to the FAA Chief Privacy Office (CPO) to ensure systems are appropriately assessed including identify privacy risk. Provides guidance to System Owners on SDA development and resolves any documentation issues; and

(3) Maintains the AIT inventory, monitors and tracks the Agency's FISMA-reportable IT inventory in the DOT FISMA Reporting System of Record, CSAM. Provides CSAM account approval for systems under AIT purview and coordinates with the account manager for the LOB for systems within their authority and tracks for the Agency. Responds to audits related to FISMA-reportable IT inventory.

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;

(2) 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;

(3) 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

(4) Conducts regulatory Privacy Compliance Assessment, 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 support services and coordination for cybersecurity architecture and engineering within the Security Operations Center (SOC); and

(2) 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 coordinating of vulnerability scanning, provides tactical execution of cybersecurity services by scanning for an evaluating vulnerabilities and risks;

(2) Performs vulnerability assessment scans 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);

(3) Ensures scanning request contain the required information and scanning reports are complete and concise, provides vulnerability scan reports with the Compliance Division, system owners, or other responsible parties, and provides information as needed to respond to data calls; and

(4) Supports the Agency's CDM program by providing technical solution support and vulnerability scanning tool expertise.

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 report 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: AIT Organizational Chart.

Chapter 9. Chief Data Office (ADO)

1. Chief Data Office (ADO-001). Concentrates on the opportunities, threats, capabilities, and gaps related to managing FAA information as a strategic asset and potentially a liability. 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 the authority to enforce changes in FAA IT policy and procedures as directed by the CIO. The following are the roles and responsibilities of ADO-001:

a. Enforces 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 & Strategy (ADO-010). The Staff Office facilitates enterprise data governance and ensures 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 processes are expected to behave in relation to data. The scope and focus of a data governance program functions:

a. Defines, communicates, and drives execution of the FAA data strategy and data governance strategy;

b. Sets polices related to data and metadata management, access, usage, and quality (security aspects are currently covered under FAA Cyber Security Orders);

c. Sets data quality and data architecture standards;

d. Provides hands-on observation, audit, and correction in key areas of quality, policy, and data stewardship;

e. Establishes governance metrics and ensures the agency can meet data-related regulatory compliance requirements;

f. Identifies, defines, escalates, and resolves issues related to data security, data access, data quality, regulatory compliance, policy, standards, terminology, or data governance procedures;

g. Sets standards and processes to consistently define the mission/business value of data assets;

h. Facilities FAA's compliance with Open Government Data Act, Geospatial Data Act and related guidance from OMB; and

i. Oversees and manages the FAA's data governance framework, which includes enterprise guidance and standards to support a federated approach.

4. Data Access & Stewardship Division (ADO-100). Works to ensure data assets are discoverable, accessible, and easy to integrate to support systems and business functions across the FAA. As business requirements evolve and technology refreshes are needed, this Division will evaluate new technologies and data products to address these needs, while exploring solutions that integrate with existing products.

a. Data Access & Stewardship Division (ADO-110):

(1) Matures enterprise-wide data governance practices, with a focus on improving data quality and the protection of sensitive data through modifications to organizational behavior, standards, processes and data architecture;

(2) Facilities the implementation of metadata standards, data quality standards, data protection standards and adoption requirements across the enterprise;

(3) Collaborates with data governance communities to enforce data standards and ensures single source of truth and data integrity for reporting and decision making;

(4) Works with data stewards and consumers to evangelize and apply data management practices to ensure data is being used in the most effective way to drive value creation;

(5) Collaborates with data governance communities and analytical teams to identify data assets to support integrated analysis;

(6) Works with data stewards, data architects, and data engineers to ensure that governed and curated data assets are made available for the wider enterprise;

(7) Promotes the numerous assets available across the agency;

(8) Enforces metadata standards to ensure data stewards deliver quality and informative metadata to enable ease of use; and

(9) Coordinates external access to data.

b. Data Platforms Branch (ADO-120):

(1) Enables self-service analytics through improving data discovery and access to data;

(2) Optimizes onboarding processes to enable timely access to data assets;

(3) Collaborates and advises program offices interested in leveraging the platform product and services throughout the Acquisition Management System (AMS) process; and

(4) Works with key stakeholders to refine business and cost models for leveraging platform.

5. Business Intelligence (BI) and Analytics Enablement Division (ADO-200). Collaborates with business partners to help the agency drive value from data and advanced analytics, which includes expanding the use of analytical techniques and solutions.

a. Analytics Enablement Branch (ADO-210):

(1) Plays a critical role in executing the mission of the Advanced Analytics Center for Enablement;

(2) Accelerates adoption of artificial intelligence by identifying opportunities for exploration, advising project teams, and supporting targeted use cases;

(3) Assists the agency in defining an enterprise artificial intelligence strategy to include cataloging use cases, sharing MLOps best practices, and establishing a model registry;

(4) Engages in user groups and governance communities to explore uses of data to meet business objectives;

(5) Sets standards and promotes best practices across business intelligence & analytics community;

(6) Works with Product Managers to improve user experience and evaluate future enhancements to meet user community needs;

(7) Performs testing and validation of newly onboarded data sets for the Data Platforms Branch; and

(8) Oversees the design and delivery of reports and insights around business functions.

b. Tools & Technology Branch (ADO-220):

(1) Accelerates adoption of advanced analytics and artificial intelligence by identifying needed tools and technology for enterprise use;

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

(3) Defines the customer segments the product will target, to understand those customers' goals, and how they would gain value from product capabilities;

(4) Facilities 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) 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);

(6) Works with key stakeholders to prioritize and schedule operations and maintenance (O&M) and enhancements;

(7) Works with key stakeholders to develop and refine business and cost models for product use, when needed; and

(8) Collaborates with Analytics Enablement and Data Platforms team to improve user experience.

6. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

Chapter 10. Administration

1. Organizational Chart. The organization chart is available on the MyFAA employee website: AIT Organizational Chart.

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. Directive Feedback Form

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 1100.171 – Office of Information and Technology (AIT) Organization (OPR: ASP-110)

To: Directives Management Officer, ASP-001

(Please mark all appropriate line items.)

☐ An error (procedural or typographical) has been noted in paragraph Click here to enter text. on page Click here to enter text.

☐ Recommend paragraph Click here to enter text. on page Click here to enter text. be changed as follows:
(Attach separate sheet if necessary.)

Click here to enter text.

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

Click here to enter text.

☐ Other comments:

Click here to enter text.

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

Submitted by: _____ Date: _____

Telephone Number: _____ Routing Symbol: _____

FAA Form 1320-19 (08/21) Supersedes Previous Edition