U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

ORDER 1375.1F

Effective date:
11/04/2021

SUBJ: Data and Information Management Policy

The Federal Aviation Administration (FAA) is committed to providing the safest, most efficient aerospace system in the world. Every day, the FAA uses significant volumes of data and information to fulfill this mission. Data and information are enterprise assets that are relied upon by the agency, industry stakeholders, global stakeholders, and the public. Therefore, this Order was founded on the *M-19-18: Federal Data Strategy – A Framework for Consistency* core principles of Ethical Governance, Conscious Design, and Learning Culture to promote proactive governance and management of data and information at the FAA.

The FAA recognizes the need for publicly available, discoverable, and usable data to support public needs like evidence-based policymaking. As the agency transitions to an open data environment, it is critical that controlled, privacy, sensitive, and unclassified critical infrastructure data and information are protected. This Order aligns the FAA with the *Open, Public, Electronic, and Necessary (OPEN) Government Data Act*, while simultaneously ensuring awareness and compliance with Federal, departmental, and agency policy and regulation to protect data and information from uncontrolled release to persons outside the FAA, and from indiscriminate dissemination within the FAA.

Finally, this Order encourages an agency culture where data and information are made discoverable and accessible to FAA personnel across Lines of Business (LOBs) and Staff Offices (SOs). As data and information become increasingly accessible within the agency, it is critical that FAA employees and contractors are keenly aware of and uphold the duty to protect FAA data and information. By creating an environment where data and information are accessible, maximally secured, and protected, the FAA can fully leverage the power of its data and information.

Steve Dickson
Administrator

Table of Contents

Chapter 1. General Information

1. Purpose of This Order. The purpose of this Order is to establish policy for:

a. Managing and governing data and information as an enterprise asset;

b. Planning and designing data and information with consideration for its current and future enterprise uses;

c. Describing, assessing, and tracing data and information throughout its lifecycle for quality and accountability;

d. Collecting, creating, and enhancing data and information for shared use;

e. Sharing and protecting data and information to create accessibility without compromising security or privacy; and

f. Retaining and disposing of data, information, and associated metadata that are considered a record.

2. Audience. This policy is for anyone who collects, develops, manages, analyzes, distributes, maintains, or authorizes the use of data and information on behalf of the FAA. FAA employees and contractors at all levels must ensure that all data and information managed, generated, collected, or acquired by or on behalf of the FAA adheres to the requirements of this Order.

3. Compliance. For assistance in complying with any provision or requirement listed in this document, please contact the Chief Data Office at 9-EIM-InfoLink@faa.gov.

4. Where to Find This Order. This Order can be found on the MyFAA website (https://employees.faa.gov/tools_resources/orders_notices/). This Order is available to the public on the FAA website (https://www.faa.gov/regulations_policies/orders_notices/).

5. What This Order Cancels. FAA Order 1375.1E, Information/Data Management, dated November 16, 2011, is canceled.

6. Scope. This policy applies to all FAA data and information (including National Airspace System [NAS] and Mission Support) that is managed, generated, collected, or acquired by the FAA or by other parties under contract on behalf of the FAA, excluding geospatial data. For policy and guidance related to geospatial data, refer to the *Geospatial Data Act of 2018*.

In addition to the requirements stated in this policy, all data and information generated, collected, or acquired by or on behalf of the FAA must adhere to existing FAA, Department of Transportation (DOT), and Federal policies and guidance relative to data and information management. See Appendix C *References.*

Information security, privacy, and the protection of Sensitive Unclassified Information (SUI), Controlled Unclassified Information (CUI), classified data and information, and otherwise restricted data and information are outside the scope of this policy. However, they are important

components of data governance and management. Therefore, “Chapter 2. Section 7. Protecting” is included in this policy to articulate information security, protection, and privacy as part of the data and information management process.

Policy references are provided for all requirements in this Order pertaining to information security, protection, and privacy. All activities conducted in compliance with this policy must also satisfy the requirements of Federal, departmental, and agency policy and regulation pertaining to the protection of SUI, CUI, Personally Identifiable Information (PII), classified data and information, or otherwise restricted data and information.

For specific requirements pertaining to the security, privacy, and protection of data and information, please reference the following policies (as amended):

a. FAA Order 1200.22, *External Requests for National Airspace System (NAS) Data*

b. FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*

c. FAA Order 1600.2, *Safeguarding Classified National Security Information*

d. FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*

e. Air Traffic Organization (ATO) Security Requirements

f. DOT Cybersecurity Compendium Supplement to DOT Order 1351.37, *Departmental Cybersecurity Policy*

Certain roles in this policy resemble but do not precisely align with those of FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*. For example, FAA Order 1370.121 uses the term “Information Owner or Steward” which closely aligns with National Institute of Standards and Technology (NIST) information security guidance. However, FAA Order 1375.1F uses the term “Steward” to be inclusive of both data and information. The Chief Data Office and Office of Information Security are aware of these discrepancies, and are working together to clarify the roles and responsibilities of both policies.

This Order does not apply to Freedom of Information Act (FOIA) requests or any external releases under any additional circumstances where release is required by law. For policy and guidance related to FOIA requests, refer to FAA Order 1270.1, *Freedom of Information Act Program (FOIA)*, as amended.

7. Explanation of Policy Changes.

a. Establishes principles and concepts to support strategic management of data and information throughout its lifecycle;

b. Establishes the role of the Chief Data Officer (CDO) and the Chief Data Office to lead the enterprise in managing and governing data and information as strategic assets;

c. Establishes the role of the Enterprise Information Management Steering Committee (EIMSC) as a cross-organizational executive group to provide leadership, advocacy, and strategic decision-making authority related to data and information management;

d. Establishes the roles of governance communities for supporting the implementation of data and information management;

e. Removes the Information and Data Advisory Board (IDAB) and distributes the responsibilities across the CDO, EIMSC, Chief Data Office, Stewardship Communities of Practice (SCoPs), Communities of Interest (COIs), and Communities of Practice (COPs); and

f. Aligns policy with *OPEN Government Data Act*, *M-19-18: Federal Data Strategy – A Framework for Consistency*, *M-13-13: Open Data Policy – Managing Information as an Asset*, and other relevant Federal policies and mandates.

Chapter 2. FAA Policy

This chapter provides data and information management requirements that align the FAA with agency, departmental, and Federal data and information management strategy and regulatory requirements. The requirements in this chapter are organized by topic.

1. Managing and Governing

a. Data and information that is created, collected, or acquired to support a program, service, application, product, capability, or otherwise fulfill the business and mission of the FAA is considered an enterprise asset.

b. Data and information have shared value across the agency, and must be managed and governed strategically. While data and information may originate within or be maintained by a specific FAA organization, it may provide value and uses to other FAA organizations in support of mission objectives.

c. In order to foster a data and information-driven culture, the FAA must recognize that data management and information management are not singularly an information technology (IT) or business responsibility, but a shared responsibility across the agency.

d. The FAA employs a federated data governance model consisting of three levels - strategic, tactical, and operational.

e. At the strategic level, the CDO and the EIMSC provide strategic guidance and oversight for initiatives pertaining to enterprise data and information management.

f. At the tactical level, the Chief Data Office works in coordination with governance communities to plan, coordinate, and execute these initiatives. Governance communities are cross-organizational groups that provide knowledge and insight on data and information management implementations and requirements (current and future). This enables the agency to standardize its data and information management practices and recommend investment decisions for common enterprise data and information management solutions and services. Governance communities are comprised of representatives from across LOBs and SOs and receive executive sponsorship from the EIMSC.

(1) SCoPs are data subject area[1] specific, technical-facing groups focused on stewardship and data architecture in support of operational and information requirements across systems, programs, and organizations.

[1] A data subject area is a logical collection of entity types based on a major resource of an enterprise. The subject area boundaries are derived by understanding data dependencies, so that logical groupings of data entity types can be identified (e.g., Airport, Navigational Aid, Employee, Aircraft, etc.).

(2) COIs are information domain[2] specific, business-facing groups focused on information requirements, information products and services, and coordination across programs and organizations.

(3) COPs are discipline[3] specific groups that collaboratively examine and define standards, best practices, and procedures to advance the understanding, value, and use of emerging technologies within that area of practice at the FAA.

g. At the operational level, stewards and custodians govern and manage data and information on behalf of their organizations, authenticating data and information content and quality.

2. Planning and Designing

a. The FAA must plan and design data and information with consideration for its current and future uses across programs, applications, products, services, and capabilities by aligning with the enterprise data and information strategy. The planning and design of data differs from that of the information system because data can move from system to system, outlive the system, or be removed before the disposal of the system.

b. The FAA must maintain an enterprise data and information strategy to enable data-driven decision-making, interoperability, innovation, and appropriate use of the FAA's data and information.

(1) The Chief Data Office is responsible for developing, coordinating, and updating the enterprise data and information strategy, and providing enterprise direction and guidance.

(2) The Chief Data Office is responsible for supporting the implementation of the enterprise data and information strategy through documentation (e.g., lifecycle management plan, quality management plan, etc.) and coordination.

(3) LOBs and SOs are responsible for defining enterprise data and information policies, practices, processes, standards, and requirements in coordination with the Chief Data Office, SCoPs, COPs, and COIs to align with the enterprise data and information strategy.

(4) LOBs, SOs, and Program Offices are responsible for adhering to the requirements of this policy when planning and designing new data and information for programs, applications, products, services, and capabilities.

c. LOBs, SOs, and Program Offices are responsible for ensuring that data and information for existing programs, applications, products, services, and capabilities adhere to the requirements laid out in this policy, as determined feasible by the respective governing body, such as the Joint Resource Council (JRC) or Operations Governance Board (OGB).

[2] An information domain is the scope of the integrated data for a distinct set of business activities that produce a set of unique information products and services (e.g. Aeronautical, Aviation Safety, Weather, Surveillance, etc.).
[3] A discipline is a field of knowledge that is taught and researched as part of the standardization and education processes (e.g. Business Intelligence & Analytics, Software Engineering, Project Management, etc.).

d. New collections of data or information may need to be approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA). If a new collection of data or information is initiated, consult with the FAA PRA Office.

3. Describing, Assessing, and Tracing. The FAA must ensure the quality and traceability of data and information throughout its lifecycle by:

a. Assigning stewards and custodians to model and define the pedigree, lineage, and metadata of the data and information. Metadata must sufficiently describe data and information to enable its reuse. Please contact 9-EIM-Infolink@faa.gov for a copy of the *FAA Metadata Standard*[4];

b. Assessing data quality regularly to ensure that it meets FAA data quality standards. Please contact 9-EIM-Infolink@faa.gov for a copy of the *FAA Data Quality Whitepaper*[5];

c. Maintaining an inventory of data and information assets and cataloging the assets and appropriate metadata to the FAA Data Governance Center (DGC), which is the FAA's enterprise data catalog to support data and information discovery and usability;

d. Maintaining the integrity of data and information from its authoritative source or approved replicated source; and

e. Reconciling known data quality and traceability issues.

4. Collecting, Creating, and Enhancing

a. Prior to collecting or creating new data and information, the FAA must seek to leverage data and information that might already exist within the FAA, another Federal entity, a non-Federal entity (such as a state or local government), or a commercial source, where practicable. FAA personnel can use the DGC to discover data and information assets that already exist within the FAA.

b. Where practicable, the FAA must collect or create data and information in machine-readable[6] and open formats[7].

c. Upon collecting or creating data and information, the steward must ensure that this data and information is fully defined with the appropriate metadata as determined by the *FAA Metadata Standard*.

[4] The *FAA Metadata Standard* is a set of common core metadata attributes based on Project Open Data Metadata Schema, as well as federal, international, and industry metadata standards.
[5] The *FAA Data Quality Whitepaper* describes how to assess data quality through the establishment of a Quality Management System.
[6] For example, XML, JSON, etc.
[7] Structured in a way that enables the data to be fully discovered by end users (*M-13-13: Open Data Policy – Managing Information as an Asset*) and fully processed with at least one open-source software tool with no restrictions placed upon its use (*Open Knowledge Foundation*)

d. The Chief Data Office is responsible for the management of the FAA enterprise metadata standards. Proposed metadata requirements must be created and coordinated with the Chief Data Office.

5. Sharing within the FAA

a. The FAA will share data and information across LOBs and SOs to the extent possible, subject to privacy[8], confidentiality, and other applicable restrictions, to enable data-driven decision-making, interoperability, and the enhancement of products and services.

b. Prior to sharing[9] data and information within the FAA, the steward must:

(1) Define the appropriate data access controls and role-based requirements for that data and information. Memoranda of Agreement (MOA) and Memoranda of Understanding (MOU) may be grandfathered as necessary; and

(2) Ensure that processes are in place to review and evaluate the appropriate protection, quality, documentation, and traceability of the released data and information.

6. Sharing external to the FAA

a. The FAA will maintain a presumption in favor of openness with respect to data and information to the extent permitted by law and subject to security, privacy, confidentiality, applicable FOIA exemptions, and other Federal, departmental, and agency policies and restrictions.

b. The FAA must publish data and information cleared for public release in machine-readable formats as soon as practicable following its collection, subject only to the limits imposed by resources, technology, data quality, and regulatory requirements, while protecting security, privacy, and confidentiality.

c. The FAA will use the FAA Data Portal as the authorized public access point for data and information cleared for public release. The FAA must prevent direct connections to FAA systems, and seek disestablishment of any unauthorized access points, where applicable. See FAA Order 1370.121, *FAA Information Security and Privacy Program Policy*, as amended.

d. The FAA must ensure that requests for NAS data are reviewed by all applicable configuration management and data release boards to ensure the security of the NAS as critical infrastructure is maintained.

e. The FAA must follow the NAS Data Release Board (NDRB) process for any NAS data set intended to be shared outside the FAA. Security issues identified with a NAS dataset during NDRB review must be resolved to the satisfaction of all associated NDRB security offices before being shared outside of the FAA. See FAA Order 1200.22, *External Requests for National Airspace System (NAS) Data*, as amended.

[8] See FAA Order 1370.121, *Information Security and Privacy Program Policy*, as amended.
[9] Disseminating data and/or information to an individual/organization other than the steward.

f. The FAA must document and coordinate data and information containing PII with the Chief Privacy Office before it is shared to ensure that any required de-identification adequately protects the original identities. See FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended.

g. The FAA will establish NIST Special Publication (SP) 800-47 compliant data and information sharing agreements with trusted partners to continuously improve, innovate, and promote safe and efficient air traffic operations or mission requirements. Trusted partners include both public and private, national and international organizations. Examples of trusted partners include Air Navigation Service Providers (ANSP) and Federally Funded Research and Development Centers (FFRDC), wherein the FAA benefits from sharing resources, technological advances, and expertise.

(1) External data and information sharing agreements established as part of a trusted partnership must fully comply with Federal, departmental, and agency policy and regulations pertaining to the protection of sensitive, classified, privacy, and otherwise restricted data and information. For a list of these policies, see Chapter 1. Section 6. Scope. For more information about these policies, see Chapter 2. Section 7. Protecting.

(2) The FAA must follow the NDRB process for external data release before sharing NAS data or information with a trusted partner.

(3) The FAA must follow international data sharing processes before establishing external data and information sharing agreements or sharing NAS data and information with international entities through trusted partnerships.

7. Protecting

a. All FAA employees and contractors have a duty to protect and safeguard the agency's data and information for the purpose of protecting national and private interests, including honoring copyright, international and tribal agreements, confidentiality, privacy, trade secrets, and compliance with other statutory and regulatory requirements.

b. Data and information containing Classified National Security Information (CNSI) must be handled, safeguarded, and shared in accordance with FAA Order 1600.2, *Safeguarding Classified National Security Information*, as amended.

c. Data and information that is SUI[10] or CUI[11] must be protected, handled, and disposed of according to the following policies, as amended: FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*, FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, *ATO Security Requirements*, and the *DOT Cybersecurity Compendium Supplement to* DOT Order 1351.37, *Departmental Cybersecurity Policy*.

[10] SUI may not always be marked as SUI. FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)* provides guidance on what types of data and information the FAA considers SUI and on how SUI must be protected.
[11] ASH is revising FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)* from SUI to CUI. For more information on designating, handling, and decontrolling information that qualifies as CUI, see *32 Code of Federal Regulations (CFR) Part 2002 – Controlled Unclassified Information.*

d. Data and information containing PII must be documented and coordinated with the Chief Privacy Office before it is shared to ensure that any required de-identification adequately protects the original identities. See FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended.

e. Data and information that is export controlled must be protected and handled in accordance with FAA Order 1240.13, *FAA Export Control Compliance*, as amended.

f. Data and information contained on low, moderate, or high impact level FAA information systems must be protected, handled, and disposed of according to the cybersecurity controls specified in FAA Order 1370.121, *Information Security and Privacy Program & Policy*, as amended.

8. Retaining and Disposing

a. Data and information that constitutes a "record" under the Federal Records Act must be properly managed. Records covered by a record schedule approved by the National Archives and Records Administration (NARA) must be disposed of in accordance with the disposition periods noted in the respective records schedule, unless subject to a litigation hold notice or preservation notice. Records pending the approval of an agency record schedule must be treated as permanent records until NARA approves the schedule. See FAA Order 1350.14, *Records Management*, as amended.

b. Data assets, including datasets and databases, that are no longer in an active production environment must be copied and stored as determined by their data lifecycle management plan until they are needed again in active production, or decommissioned.

c. When a data or information asset is deemed decommissioned, the steward must coordinate the removal of all copies of the asset from the FAA with their LOB/SO Records Liaison Officer (RLO) or Service Office/Service Unit Records Liaison Officer (RLO-S) to prevent inadvertent use of the asset.

Chapter 3. Roles and Responsibilities

1. Strategic Level

a. FAA Chief Information Officer (CIO): The senior agency official that is responsible for managing all aspects of information technology within the FAA, including cybersecurity, privacy requirements, and safeguards of all FAA systems. The CIO leads the Office of Information Technology (AIT). The CIO has the authority to delegate responsibilities to the FAA CDO. The responsibilities of the CIO[12] pertaining to this policy include:

(1) Promoting enterprise data and information management concepts and the enterprise data and information strategy;

(2) Providing the agency with tools to manage and govern its data and information assets; and

(3) Sponsoring training programs for data and information management and governance practices.

b. FAA Chief Data Officer (CDO): The senior agency official that is primarily responsible for operationalizing the vision that data and information are strategically managed as enterprise assets. This means improving links between databases and data stores, making data and information easier to find in open and machine-readable formats, and making it easier for analysts and policymakers to quickly access and transform data into new formats and knowledge. The CDO leads the Chief Data Office and reports to the CIO. The general responsibilities of the CDO include:

(1) Engaging agency employees, contractors, and industry partners on the data and information management concepts and the enterprise data and information strategy;

(2) Guiding and overseeing enterprise data governance, standardizing data formats and information within the FAA and with domestic and international partners, increasing visibility into available agency data sets with secure, role-based access controls to optimize FAA operations, and the development of enterprise data quality standards;

(3) Coordinating with agency officials responsible for using, protecting, disseminating, and generating data;

(4) Enhancing the use of advanced and sophisticated analytic technologies that foster growth in the agency's decision-making capabilities;

(5) Establishing an enterprise environment of common practices and shared resources that support rapidly changing business needs in a strategic, cost-effective way; and

[12] The responsibilities of the CIO pertaining to information security are explained in FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended.

(6) Educating and empowering the workforce through training, tools, data and information governance communities, and other opportunities to expand data management and analytics capabilities.

c. Enterprise Information Management Steering Committee (EIMSC): A cross-organizational group of senior agency officials who represent their LOBs and SOs regarding the enterprise implementation of data and information management. The EIMSC is responsible for making decisions about the prioritization and pursuit of strategic initiatives pertaining to enterprise data and information management. The EIMSC is chaired by the CDO. The general responsibilities of the EIMSC include:

(1) Directing and overseeing the design, development, and implementation of enterprise data and information policies, processes, operational practice, and procedures used in the capture, representation, exchange, and analysis of data and information;

(2) Engaging FAA leaders and programs to ensure that organizational needs are considered during enterprise data and information management implementation; and

(3) Reviewing the agency's data and information governance frameworks to improve collaboration, efficiency, and effectiveness.

d. FAA Chief Privacy Officer (CPO): The senior agency official that provides expertise and oversight for privacy requirements across the Information Security and Privacy service areas and the enterprise in accordance with the *Privacy Act of 1974*, the *E-Government Act of 2002*, the *Federal Information Security Modernization Act of 2014* (*FISMA*), and policy and guidance issued by the White House and the Office of Management and Budget. The CPO role is within the Information Security and Privacy Service (AIS) under AIT. The general responsibilities of the CPO include:

(1) Implementing accountability and continuous improvement of FAA privacy processes and programs;

(2) Reviewing privacy compliance documentation inclusive of Privacy Threshold Assessments (PTA), Privacy Impact Assessments (PIA), System Disposal Assessments (SDA), and provides updates to System of Records Notice (SORN) for adjudication by DOT; and

(3) Providing guidance for the protection of PII and records, and for compulsory terms involving privacy data.

e. System Operations Security (AJR-2): The Office of Primary Responsibility (OPR) for the NAS Data Release Board (NDRB). Authorized and held accountable by the ATO Authorizing Official (AO) for the identification and protection of Sensitive Flight Data (SFD) across the enterprise. *SFD has status as SUI.* The general responsibilities of AJR-2 include:

(1) Managing the NDRB to adjudicate requests for external release of NAS data;

(2) Providing expertise and oversight for SFD protection wherever it may exist; and

(3) Providing direction on confidentiality protection requirements for SFD.

f. NAS Security and Enterprise Operations (AJW-B): The organization authorized and held accountable by the ATO Authorizing Official (AO) for the identification and protection of ATO Cybersecurity Authorization and Vulnerability Information (CAVI) and NAS Sensitive Technical Information (STI) across the enterprise. *ATO CAVI and NAS STI have status as SUI*. The general responsibilities of AJW-B include:

(1) Providing expertise and oversight for ATO CAVI and NAS STI protection wherever it may exist; and

(2) Providing direction on confidentiality protection requirements for ATO CAVI and NAS STI.

g. Designated Agency Records Officer (**ARO**): The person assigned responsibility by the agency head for overseeing an agency-wide records management program. The ARO has the authority to delegate RIM tasks requiring ARO approval to FAA RIM Program Office staff. The ARO role is within Strategy & Performance Service (ASP) under AIT. The general responsibilities of the ARO include:

(1) Serving as the FAA's primary point of contact for RIM concerns and implementation of the Agency's RIM program. See FAA Order 1350.14, *Records Management*, as amended;

(2) Developing Agency procedures, records retention schedules, directives and other RIM tools consistent with NARA, DOT and FAA policies; and

(3) Interpreting RIM statutes, regulations, and other legal requirements affecting the Agency's RIM Program and ensuring agency compliance.

h. FAA Freedom of Information Act (FOIA) Program Manager: The person assigned responsibility by AFN-1 for overseeing an agency-wide FOIA Program. The general responsibilities of the FOIA Program Manager include:

(1) Serving as the FAA's primary point of contact for FOIA concerns and implementation of the Agency's FOIA program. See FAA Order 1270.1, *Freedom of Information Act (FOIA) Program*, as amended;

(2) Developing Agency policy, procedures, and guidance consistent with FOIA, *5 U.S.C. 552*, and DOT regulations found in *49 CFR Part 7 – Public Availability of Information*; and

(3) Interpreting FOIA statutes, regulations, and other legal requirements affecting the Agency's FOIA program and ensuring compliance.

i. NAS Enterprise Architecture and Requirement Services (ANG-B1): The organization responsible for the NAS Enterprise Architecture Models, including Data and Information Architecture Models, and Requirement Development, and Maintenance. The general responsibilities of NAS Enterprise Architecture and Requirement Services include:

(1) Supporting SCoPs in data modeling efforts;

(2) Serves as the Concept and Requirement Definition (CRD) Lead, the liaison to the Acquisition System Advisory Group (ASAG) and Verification and Validation (V&V) Strategies and Practices Branch, and the champion for the Integrated Planning Committee (IPC); and

(3) Engages and collaborates across all LOBs, SOs, and the FAA Systems Engineering (SE) community to promote SE services, data, products, and best practices.

2. Tactical Level

a. Chief Data Office: An organization that works in coordination with governance communities, LOBs, and SOs to support the implementation of enterprise data and information management and governance solutions. The Chief Data Office is led by the CDO. The general responsibilities of the Chief Data Office include:

(1) Coordinating with SCoPs, COIs, and COPs to facilitate the development of enterprise data and information standards and solutions;

(2) Developing, coordinating, and updating the enterprise data and information strategy, and providing enterprise guidance and direction;

(3) Providing and promoting resources, tools, techniques, and processes for governing and managing data; and

(4) Reporting progress and escalating risks to the CDO or EIMSC, as necessary.

b. Stewardship Communities of Practice (SCoP): Governance communities that are specific to a data-subject area as defined by the FAA Enterprise Data Architecture. SCoPs are focused on stewardship and data architecture in support of operational and information requirements across systems, programs, and organizations. Through data architecture, SCoPs ensure the data and its attributes support the "As-Is" and "To-Be" requirements of the business and its operations. LOBs and SOs coordinate with the Chief Data Office to request SCoP establishment and provide representatives to serve as SCoP sponsors, chairs, and members. The EIMSC approves the establishment of SCoPs and provides oversight. The general responsibilities of a SCoP include:

(1) Analyzing and managing the baseline and change control of the FAA Enterprise Data Architecture and managing integrated transition plans ("As-Is" to "To-Be") within their data subject area;

(2) Facilitating the registration of data assets in coordination with the Chief Data Office to ensure quality, integrity, proper lineage and pedigree, and accurate descriptions for discoverability and usability purposes;

(3) Reviewing change requests, new requirements, and analyses pertaining to FAA data that fall within their data subject area;

(4) Managing interdependencies, integrated transition plans, formal arrangements around data, and role-based access controls; and

(5) Ensuring interoperability across FAA LOBs, SOs, and data subject areas.

c. Communities of Interest (COI): Governance communities that are business-facing and specific to an information domain as defined by the FAA Enterprise Information Architecture. COIs are focused on information requirements and coordination across programs and organizations. COIs receive requirements, problem statements, and needs for products and services, external partners, external organizations, and programs, and communicate these requirements to SCoPs as necessary. LOBs and SOs coordinate with the Chief Data Office to request COI establishment and provide representatives to serve as COI sponsors, chairs, and members. The EIMSC approves the establishment of COIs and provides oversight. The general responsibilities of a COI include:

(1) Reviewing the analyses and recommendations provided by working groups pertaining to their information domain;

(2) Identifying, defining, and satisfying the information needs of end users and business activities within their information domain;

(3) Determining strategic activities and viable plans for transitioning to the desired future state;

(4) Communicating changes to requirements, standards, or enhancements to the appropriate SCoP;

(5) Managing the baseline and change control of the FAA Enterprise Information Architecture structure for initiatives within their information domains;

(6) Identifying and contributing metadata to the DGC for information products within their information domain; and

(7) Ensuring interoperability across FAA LOBs/SOs and information domains.

d. Communities of Practice (COP): Governance communities comprised of practitioners who share a specific discipline and collaboratively examine and define standards, best practices, and procedures to advance the understanding, value, and use of emerging technologies within that area of practice at FAA. COPs advise COIs and SCoPs on the implementation of these standards and practices. LOBs and SOs coordinate with the Chief Data Office to request COP establishment and provide representatives to serve as COP sponsors, chairs, and members.

The EIMSC approves the establishment of COPs and provides oversight. The general responsibilities of a COP include:

(1) Testing emerging technologies within their discipline and providing feedback and recommendations for use within the FAA;

(2) Reviewing and collaborating on industry standards and best practices within their discipline;

(3) Defining standards and best practices for the FAA within their discipline; and

(4) Advising SCoPs and COIs on the implementation of these standards and best practices.

e. Data Architect: Individuals responsible for the FAA Enterprise Data Architecture, which includes logical, physical, and canonical models and policies, rules, and standards that govern data collection and disposal. Data architects support standardized interoperability through the strategic planning of data across systems, platforms, and organizations. The general responsibilities of a Data Architect include:

(1) Working with SCoPs and program offices to describe, model, integrate, define structure, govern, store, and maintain data in the enterprise for accuracy and enterprise usage;

(2) Supporting policies and procedures enforced by the Chief Data Office to ensure best practices of data architecture including accountability, governance, and requirements;

(3) Fostering enterprise operational use of data and information for business process functions by analyzing how information should flow and be consumed to carry out enterprise operational capabilities; and

(4) Documenting data inventory in the DGC to determine what can be measured, when, and how.

f. Information Architect: Individuals responsible for the development and maintenance of the FAA Enterprise Information Architecture. The general responsibilities of an Information Architect include:

(1) Maintaining a working knowledge of strategies, business capabilities, increments, and new initiatives;

(2) Pulling subsets of data from authoritative sources of different data subject areas together to answer a business need (for example, discovery, analytics, information product, orchestrated services); and

(3) Developing and maintaining the FAA Enterprise Information Architecture by organizing, structuring, and labeling content using search schemas, thesauri, metadata, taxonomies, ontologies, and business processes in an effective and sustainable way to help consumers find information to complete tasks.

3. Operational Level

a. Steward: Individuals or groups designated by an organization where data or information originates, who are accountable for the quality, timeliness, protection, and access of that data or information, and are responsible for the metadata about the authoritative source. The general responsibilities of a steward include:

(1) Providing input and working closely with the System Owner, Information System Security Managers (ISSM) or Authorizing Official (AO), Servicing Security Elements (SSE), and the LOB/SO Privacy Office to establish the appropriate handling, control, security, and protection requirements for authoritative source data and information. See FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended;

(2) Reviewing and adjudicating internal requests to authoritative source data in a timely manner;

(3) Maintaining a record of users that are authorized to access authoritative source data;

(4) Adopting and implementing procedures and processes for governing the generation, collection, processing, dissemination, archival, and disposal for authoritative source data;

(5) Validating and ensuring the quality of data and information in the authoritative source and resolving content and quality issues;

(6) Ensuring that the authoritative source metadata complies with *the FAA Metadata Standard*;

(7) Ensuring that the authoritative source and its metadata, including the pedigree and lineage, are accounted for in the DGC;

(8) Clearly and concisely defining and representing business information and data requirements for the collection of data and information to support its operational use;

(9) Participating in data and information governance communities as applicable to provide subject matter expertise to improve enterprise information knowledge and sharing;

(10) Providing requirements for internal and external data exchanges of authoritative source data and information; and

(11) Managing access controls and formal arrangements, to include Statements of Work (SOW), Service Level Agreements (SLA), Letters of Agreement (LOA), Memorandums of Understanding (MOU), and Interoperability Agreements (IA) as needed.

b. Custodian: Individuals or groups designated by an organization with data or information that has been transformed or replicated for a business need, who is responsible for the integrity, pedigree, and lineage of the approved replicated source. Custodians are accountable for proper handling of the data or information they receive by upholding policies and regulations governing its use, in accordance with agreements made with the respective steward. When the steward is

external to the FAA, a custodian must quality control and audit the data or information prior to making it available in the FAA authoritative source. In this case, a custodian will work with the external steward to make any necessary corrections. The general responsibilities of a custodian include:

(1) Providing input and working closely with the steward, system owner, Information System Security Managers (ISSM) or authorizing official (AO), Servicing Security Elements (SSE), and the LOB/SO Privacy Office to establish the appropriate handling, control, security, and protection requirements for the transformed or replicated data or information. See FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended;

(2) Adopting and implementing procedures and processes for governing the generation, collection, processing, dissemination, archival, and disposal for the approved replicated source;

(3) Ensuring that the approved replicated source metadata complies with the *FAA Metadata Standard*;

(4) Ensuring that the approved replicated source and its metadata are accounted for in the DGC;

(5) Clearly and concisely defining and representing business information and data requirements for the collection of replicated data and information to support its operational use;

(6) Ensuring the integrity of the approved replicated source data and information received from the authoritative source by performing validation and verification processes and procedures; and

(7) Communicating and resolving data and information content issues with the steward.

Chapter 4. Administrative Information

1. Distribution. This Order is available electronically on the MyFAA employee website at: (https://employees.faa.gov/tools_resources/orders_notices/). This Order is available to the public on the FAA website (https://www.faa.gov/regulations_policies/orders_notices/)

2. Authority to Change This Order. The issuance, revision, or cancellation of the material in this Order is the responsibility of the Chief Data Office. The Administrator delegates the authority and responsibility to the Chief Information Officer to establish policy and standards, assign organizational and management responsibilities to the CDO, and oversee Agency compliance of Federal laws, policies, standards, and regulations about data and information management.

3. Suggestions for Improvements. Please forward all comments on deficiencies, clarifications, or improvements regarding the contents of this Order to the Chief Data Office at 9-EIM-InfoLink@faa.gov. Your suggestions are welcome. FAA Form 1320-19, *Directive Feedback Information*, is located in Appendix D of this Order for your convenience.

4. Records Management. Refer to FAA Order 0000.1, *FAA Standard Subject Classification System*; FAA Order 1350.14, *Records Management*; or your office Records Liaison Officer (RLO)/Directives Management Officer (DMO) for guidance regarding retention or disposition of records.

Appendix A. Definitions

Approved Replicated Source: A designated repository with properly documented pedigree and lineage metadata traceable to an authoritative source fulfilling a specific business purpose, updated concurrently with updates to the authoritative source. Data or information replicated from an authoritative source is read-only.

ATO Cybersecurity Authorization and Vulnerability Information (CAVI): Information concerning system security measures, which is largely generated as part of the process of conducting regular cybersecurity assessments and authorizations (e.g., cybersecurity authorization documentation, vulnerability scan results).

Authoritative Source: The designated repository (primary source) for data or information provided by the steward.

Controlled Unclassified Information (**CUI**): Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by, or for, an executive branch agency or an entity acting for an agency.

Custodian: An individual designated by an organization with data that has been transformed or copied for a business need, who is responsible for the integrity, pedigree, and lineage of the data. Custodians are accountable for proper handling of the data they receive by upholding policies and regulations governing its use, in accordance with agreements made with the respective steward.

Data: Representation of fact, concept, or instruction in a form suitable for communication, interpretation, or processing either by humans and/or by automated systems. This is the lowest level of abstraction, compared to information and knowledge.

Data governance: A collection of policies, practices, and procedures which help to ensure the formal management of data and information. These policies, practices, and procedures create alignment between organizational goals and how data and information are managed. Examples include data quality standards, data and information policies, governance bodies, and formalized stewardship.

Data management: The implementation of policies, practices, and procedures which allow the organization to manage data and information throughout its lifecycle. Examples include data and information architecture, data and information protection, data preparation, data warehousing, and metadata management.

Data subject area: A logical collection of entity types based on a major resource of an enterprise. The subject area boundaries are derived by understanding data dependencies, so that logical groupings of data entity types can be identified (e.g., Airport, Navigational Aid, Employee, Aircraft, etc.).

Described: The use of robust, granular metadata to document the strengths, weaknesses, analytical limitation, security requirements, data elements, data dictionaries and, if applicable, the purpose of collection, the population of interest, the sample characteristics, and the method of collection for a dataset. (Adapted from *M-13-13: Open Data Policy – Managing Information as an Asset*)

Discipline: A field of knowledge that is taught and researched as part of the standardization and education processes (e.g., Business Intelligence & Analytics, Software Engineering, Project Management).

Discoverable: Making metadata available for humans to read and machines to process; the technical attributes that facilitate human and machine-readable metadata for the purposes of indexing, searching, and accessing data and information. (Adapted from *M-13-13: Open Data Policy – Managing Information as an Asset*)

Dissemination: Agency-initiated or sponsored distribution of data and information (*OMB Information Quality Guidelines*)

Enterprise data and information asset: A data and information resource is owned or controlled by the agency, which holds or produces value, or can be invested in to derive future value.

Enterprise data catalog: A centralized repository, which provides role-based access of the metadata of data and information assets to authorized users; allows users to find, understand, and locate FAA data and information assets.

FAA Enterprise Architecture: The FAA Enterprise Architecture provides an explicit description of the current and desired relationships among business and management processes and information technologies within the FAA. The Enterprise Architecture consists of business process models, technical reference models, and systems models and is directly supported by the FAA Enterprise Data Architecture.

FAA Enterprise Data Architecture: The FAA Enterprise Data Architecture is part of the FAA Enterprise Architecture and provides the blueprint of the high-level data requirements of the agency. It is a model representing data objects that are important to the enterprise. It further articulates the relationships between data objects and the principles and guidelines governing their design and evolution over time. It is also a key component of the FAA's compliance with the OMB Federal Enterprise Architecture Data Reference Model.

FAA Enterprise Information Architecture: The FAA Enterprise Information Architecture, in alignment with the FAA Enterprise Architecture, provides the blueprint of the information requirements of the agency. It is an ontology showing the dependencies between categories of information used by the business to make business decisions or initiate action. It also provides a lexicon of terms and identifies their placement within the ontology.

Information: Data in context. The meaning given to data or the interpretation of data based on its context. The finished product as a result of the interpretation of data. Data that is processed in such a way that it can increase the knowledge of the person who receives it. Data that (1) has been verified to be accurate and timely, (2) is specific and organized for a purpose, (3) is

presented within a context that gives it meaning and relevance, and (4) leads to an increase in understanding and decrease in uncertainty. The value of information lies solely in its ability to affect a behavior, decision, or outcome.

Information domain: The scope of the integrated data for a distinct set of business activities that produce a set of unique information products and services (e.g., Aeronautical, Aviation Safety, Weather, Surveillance, etc.).

Information management: The leading, planning, organizing, structuring, describing, and controlling of the collection of information (developed from one or more data sources) and monitoring that information throughout its lifecycle; including the distribution of information to one or more audiences, and reviewing user needs to incorporate future best practices.

Integrity: A degree of assurance that data and its value has not been lost or altered since the data origination or authorized amendment.

Joint Resources Council (JRC): The senior investment review board for the FAA responsible for making corporate-level investment decisions based on specified knowledge (decision criteria) the service organization or program office must provide before entry into a decision point. The JRC also oversees implementation of FAA investment programs.

Machine-readable: Data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost (e.g., XML, JSON, etc.). (Adapted from *Open Government Data Act*)

Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In the context of this policy, an MOU/A defines the responsibilities of two or more organizations for securely sharing safeguarded, sensitive data and information. (Adapted from *NIST SP800-47, Security Guide for Interconnecting Information Technology Systems*)

Metadata: Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions. (Source: *Open Government Data Act*)

National Airspace System (NAS) Data and Information: The data and information from the U.S. aviation ecosystem; Air Traffic Control (ATC) automation, surveillance, navigation, communication, weather, maintenance and operational support equipment and services; air navigation facilities; airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material directly used to ensure safe and efficient use of U.S. navigable airspace. Included is data from components shared jointly with the military and other governmental entities, and data from support environments such as training, development, testing, and security (physical, personnel, and cyber). NAS data is generated in the NAS, but may exist in any environment (NAS Operations, NAS Support, Research and Development, Mission Support, or external entity domains such as other government agencies, aviation partners, academia, and industry). It maintains its designation as NAS data regardless of the environment in which it resides, and this

designation determines the requirements for its protection, handling, and sharing.

NAS Sensitive Technical Information (STI): Data or information of a scientific or technical nature used in operation or support of the NAS (e.g., NAS IP addresses, user IDs and passwords, source or adaptation code, security logs), which an adversary might be able to use or leverage, alone or in conjunction with other information, to compromise, disrupt or interfere with the NAS or any NAS asset.

Mission Support Data and Information: The data and information needed for FAA regulatory, business administration, and planning function that are not part of the NAS. It includes all of the administrative applications, systems, and related policies and procedures not directly involved in the NAS.

Open data: Publicly available data structured in a way that enables the data to be fully discoverable and usable by end users and is consistent with the principles of public, accessible, described, reusable, complete, and timely, managed post-release. (Source: *M-13-13: Open Data Policy – Managing Information as an Asset*)

Open format: Open format refers to data that is structured in a way that enables the data to be fully discovered by end users and fully processed with at least one open-source software tool with no restrictions placed upon its use. (Adapted from *M-13-13: Open Data Policy – Managing Information as an Asset* and *Open Knowledge Foundation*)

Operations Governance Board (**OGB**): The executive body that reviews, approves, oversees, and informs the Joint Resources Council and other agency executive boards and organizations concerning mission-support operations-funded capital investments.

Personally Identifiable Information (**PII**): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, including, but not limited to; name, home address, Social Security Number, driver's license/state-issued identification number, date and place of birth, mother's maiden name, biometric records, education, financial transactions, medical information, non-work telephone numbers and criminal or employment history, etc., including any other personal information that is linked or linkable to an individual. PII requires a case-by-case assessment of the specific risk that an individual can be identified. The specifics of PII within the FAA and the NAS are defined and governed under FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended.

Records: Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. (*44 U.S.C. 3301*)

Sensitive Flight Data (SFD): Sensitive Flight Data is ***all*** flight data, inclusive of positional/track and/or identification data (i.e., call sign, aircraft type, beacon code, route of flight, etc.) generated by aircraft conducting sensitive U.S. government flight missions for the purposes of national defense, homeland security, intelligence, and law enforcement. SFD that the FAA collects from U.S. government sensitive flight missions is protected as sensitive unclassified information (SUI) and not released to the public. This protective security measure is sometimes referred to as 'FAA Security Source Blocking.' SFD is also a specific information security information type used by the FAA that must be protected at the Moderate Confidentiality level in accordance with applicable Federal information security requirements contained in FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*, as amended.

Sensitive Unclassified Information (SUI): Unclassified information– in any form including print, electronic, visual, or aural forms - which we must protect from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act (FOIA).

Service Level Agreement (SLA): An agreement between two or more parties that defines, but is not limited to, standards, timeliness, quality and documentation associated with the data and information that will be shared/disseminated.

Sharing: Disseminating data and information to an individual/organization other than the steward.

Steward: An individual designated by an organization where data and information originates, who is accountable for the quality and timeliness of that data or information, and is responsible for the metadata about the authoritative source.

Timeliness: The degree of confidence that the data is current and up to date during the period of its intended use.

Traceability: Ability to trace the history, application, or location of that which is under consideration (*International Organization for Standardization (ISO) 9000).* Traceability is formally documented through a pedigree and lineage meta-model.

Appendix B. Acronyms

AIT	Office of Information Technology
ANSP	Air Navigation Service Provider
AO	Authorizing Official
ARO	Agency Records Officer
ASAG	Acquisition System Advisory Group
ATO	Air Traffic Organization
CAVI	Cybersecurity Authorization and Vulnerability Information
CDO	Chief Data Officer
CIO	Chief Information Officer
CFR	Code of Federal Regulations
CNSI	Classified National Security Information
COI	Community of Interest
COP	Community of Practice
CPO	Chief Privacy Officer
CRD	Concept and Requirement Definition
CUI	Controlled Unclassified Information
DOT	Department of Transportation
EIM	Enterprise Information Management
EIMSC	Enterprise Information Management Steering Committee
FAA	Federal Aviation Administration
FFRDC	Federally Funded Research and Development Centers
FOIA	Freedom of Information Act
GRS	General Records Schedule
IA	Interoperability Agreement
IPC	Integrated Planning Committee
ISO	International Organization for Standardization
ISSM	Information System Security Managers
IT	Information Technology
JRC	Joint Resources Council
LOA	Letter of Agreement
LOB	Line of Business
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NAS	National Airspace System
NDRB	NAS Data Release Board
NIST	National Institute of Standards
OGB	Operations Governance Board
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Assessments
RIM	Records and Information Management

RLO	Records Liaison Officer
RLO-S	Service Unit Records Liaison Officer
SCoP	Stewardship Community of Practice
SDA	System Disposal Assessments
SE	Systems Engineering
SFD	Sensitive Flight Data
SLA	Service Level Agreement
SO	Staff Office
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
SSE	Servicing Security Elements
STI	Sensitive Technical Information
SUI	Sensitive Unclassified Information
V&V	Verification and Validation

Appendix C. References

The following references were used to develop this Order, and provide additional guidelines on the management and governance of data and information. Other Federal laws, regulations, and guidance not listed here, such as executive orders, may apply:

Number	Federal Laws, Regulations, Guidance	Location
1	FAA Order 1370.121A, Information Security and Privacy Program & Policy	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1038496
2	FAA Order 1200.22E, External Requests for National Airspace System (NAS) Data	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1019774
4	FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI)	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentid/14210
5	FAA Order 1270.1A, Freedom of Information Act Program	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentid/1027435
6	DOT Order 1351.34 Data Management Policy	https://www.transportation.gov/digitalstrategy/policyarchive/Departmental-Data-Release-Policy
8	OPEN Government Data Act	https://www.congress.gov/bill/115th-congress/house-bill/4174
9	M-19-18: Federal Data Strategy – A Framework for Consistency	https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf
10	M-13-13: Open Data Policy – Managing Information as an Asset	https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-13.pdf
11	FAA Order 1350.14B, Records Management	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1022926
12	DOT Order 1351.37, Departmental Cyber Security Policy	https://www.transportation.gov/digitalstrategy/policyarchive/Departmental-Cyber-Security-Policy

Number	Federal Laws, Regulations, Guidance	Location
13	0000.1G, FAA Standard Subject Classification System	https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/12832
14	Privacy Act of 1974	https://www.justice.gov/opcl/privacy-act-1974
15	E-Government Act of 2002	https://www.justice.gov/opcl/e-government-act-2002
16	Federal Information Security Modernization Act	https://www.cisa.gov/federal-information-security-modernization-act
17	Geospatial Data Act of 2018	https://www.fgdc.gov/gda

Appendix D. Directive Feedback Information

Directive Feedback Information

Please submit any written comments 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 1375.1F To: 9-EIM-InfoLink@faa.gov
Please mark all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph___on page___.

☐ Recommend paragraph___on page___be changed as follows:

☐ In a future change to this order, please cover the following subject:

(Briefly describe what you want added.)

☐ Other comments:

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

Submitted by:_____Date:_____

Telephone Number:_____Routing Symbol: _____

FAA Form 1320-19 (10-98)