U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Aviation Safety (AVS)

Aviation Safety Knowledge Management Environment 2 (ASKME 2) Airworthiness Directives Development (ADD)

Responsible Official

Brenda Bailey
Email: Brenda.Bailey@faa.gov

Reviewing Official

Karyn Gorman
Chief Privacy
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration (FAA) is developing this Privacy Impact Assessment (PIA) for Aviation Safety Knowledge Management Environment 2 Airworthiness Directives Development (ASKME 2 ADD). ASKME 2 ADD is a centralized database that is used by the Aviation Safety (AVS) organization for collecting and storing documents related to aircraft airworthiness. These documents include Airworthiness Directives (ADs), Mandatory Continuing Airworthiness Information (MCAIs), Special Airworthiness Information Bulletins (SAIBs), and Alternative Methods of Compliance (AMOCs). This PIA focuses on AMOCs since it is the only documentation within ASKME 2 ADD that collects Personally Identifiable Information (PII) from aircraft owners and operators. The authorities for collecting information in ASKME 2 ADD are the safety mandates of 49 United States Code (USC) § 44701 and 14 Code of Federal Regulations (CFR) Part 39.

The FAA is publishing this PIA for ASKME 2 ADD in accordance with Section 208 of the E-Government Act of 2002 because ASKME 2 ADD collects name, address, phone, email and fax number from aircraft owners and operators.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The authorities for collecting information in ASKME 2 ADD are 49 USC § 44701 and 14 CFR Part 39. ASKME 2 ADD is a centralized database that is used by the AVS organization for collecting and storing the following documents related to aircraft airworthiness. These documents include:

- Airworthiness Directive (AD) is issued by the FAA when there is an unsafe condition that is discovered on a specific aircraft, aircraft engine, propeller, or appliance and that condition exists or is likely to exist on other products of the same type design. The AD contains the FAA required method for resolving that unsafe condition. FAA Aviation Safety Engineers (ASEs) prepare the AD worksheets in ASKME 2 ADD. AD collects Design Approval Holder's (DAH)[2] full business name and business contact information, the ASE's name, business contact information (telephone number, address, and email address) and technical information about the aircraft type or product. DAH are companies not individuals.
- Mandatory Continuing Airworthiness Information (MCAI) is an airworthiness directive issued by a foreign entity that is evaluated in order for the FAA to make a determination if an FAA issued AD is needed. MCAI does not collect any PII.
- Special Airworthiness Information Bulletins (SAIB) is an information tool that alerts, educates, and makes recommendations to the aviation community. SAIBs contain non-regulatory information and guidance that does not meet the criteria for

[2] DAH means the holder of any design approval, including Type Certificates (TCssx, amended TCs, Supplemental Type Certificates (STCs), amended STCs, PMAs, technical standard order (TSO) authorization, letter of TSO design approval, and field approvals (FAA Form 337).

an AD. The SAIB includes the information DAH's or Production Approval Holder (PAH)[3] name if applicable, ASE's name, and business contact information (telephone number, address and email address), parts information and aircraft subject code. In rare instances, a DAH or PAH can be an individual; however, the FAA only collects business contact information.

- AMOC is required if an aircraft owner/operator or DAH cannot or chooses not to comply with an AD or finds a different method to comply with the actions specified in an AD. An AMOC provides an acceptable level of safety for a different way, other than the one specified in the AD, to address the unsafe condition.

The scope of this PIA discusses AMOCs since it is the only documentation within ASKME 2 ADD that collects PII for aircraft owners and operators.

The FAA requires aircraft owners or operators to resolve unsafe conditions outlined in an AD and provide an airworthiness certificate indicating that the aircraft is safe for public use. As mandated by FAA Order 8110.103B, an AMOC is required if an aircraft owner/operator or DAH cannot comply with an AD or finds a different method to comply with the actions specified in an AD. An AMOC provides an acceptable level of safety for a different way, other than the one specified in the AD, to address the unsafe condition.

The ASKME 2 ADD automates the process for submitting an AMOC request to the FAA. Users access ASKME 2 ADD at https://add.faa.gov to initiate the AMOC. Users are not required to enter a username or password to access the system. Once they agree to the system use notice, they are required to enter their name, address, city, state, country, zip code, telephone number and email address and optionally enter their company name and fax number. In addition, the user enters the affected product(s), model designation(s), serial number(s) and state of registry, to initiate an AMOC. The user describes in a free-text box what they are proposing and how their proposed AMOC resolves the unsafe condition with an acceptable level of safety. The user can edit anything on the AMOCS up to the point of submission. After the user submits the AMOC proposal, ASKME 2 ADD generates a confirmation pop-up that includes AMOC Request Identifier Number for the user. Users must contact the assigned ASE via phone call or email if changes to the proposal are needed after submission.

When AMOC requests are submitted, they are assigned to an ASE for approval or denial[4]. ASEs may edit and amend the AMOC request information within ASKME 2 ADD, if

[3] PAH is a company or legal entity that holds any one of the following approvals issued by the FAA: a production certificate (PC), an approved production inspection system (APIS), a parts manufacturer approval (PMA) or a TSO authorization.
[4] If an ASE denies the approval, the AMOC submitter is notified and provided technical data that describes why the denial is issued and how to resolve it.

applicable[5]. The ASE uploads documents that are used in the decision-making process which never contain PII. The ASE enters optional comments that explain the basis of the AMOC decision in a free-form text field, which does not contain PII.

The ASE generates the approval letter outside of ASKME 2 ADD. Prior to mailing the approval letter, the approval letters are uploaded into ASKME 2 ADD and contain the Aircraft Certification Service (AIR) Manager's name, job title and signature, name and mailing address of the AMOC requestor, AD number[6] and the specific paragraph to which the AMOC applies, the Flight Standards District Office (FSDO) location and limitations on the AMOC's applicability. If an AMOC is denied, the submitter is notified by letter that describes why the denial is issued and how to resolve it.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[7], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[8].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

[5] The ASE collaborates with the AMOC submitter to clarify areas of concern and may make edits to the AMOC with the permission of the submitter.
[6] ADs are legally enforceable regulations issued by the FAA in accordance with 14 CFR part 39 to correct an unsafe condition in a product. Part 39 defines a product as an aircraft, engine, propeller, or appliance.
[7] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[8] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

ASKME 2 ADD collects the name, address, city, state, country, zip code, telephone number and email address and optional company name and fax number of the requester. In addition, it collects affected product(s), model designation(s), serial number(s) and state of registry, to initiate an AMOC. When records are retrieved, it is done so by using information about the aircraft and are not retrieved a personal identifier. Therefore, these records do not qualify as a Privacy Act system of records. Non substantial records for user accounts are covered by DOT/ALL 13, "*Internet/Intranet Activity and Access Records,*" 67 FR 30758 May 7, 2002.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the ASKME 2 ADD.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Users can edit their AMOC up to the point of submission. After the AMOC has been submitted the user can contact the ASE and request them to make changes to their AMOC. When records are retrieved, they are about the aircraft and not an individual and therefore not subjected to the privacy act.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

ASKME 2 ADD collects the name, address, city, state, country, zip code, telephone number and email address and optional company name and fax number. In addition, it collects the affected product(s), model designation(s), serial number(s) and state of registry, to initiate an AMOC. ASKME 2 ADD a centralized database that is used by the AVS organization for collecting and storing the following documents related to aircraft airworthiness. These documents include ADs, MCAIs, SAIBs, and AMOCs. The authorities for collecting information in ASKME 2 ADD are 49 USC 44701 and 14 CFR Part 39.

ASKME 2 ADD shares PII with the following FAA internal IT systems:

Aviation Safety Knowledge Management Environment – Enterprise Services (ASKME ES) provides the name, email address and telephone number for FAA employees. This information is used to provide for user access.

Federal Aviation Administration Directory Service (FAA DS) receives the email address of employees, for the purpose of identity authentication of FAA users.

The FAA has established appropriate data-sharing instruments between FAA program offices to document data protection requirements.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

ASKME 2 ADD only collects, uses and retains PII that is relevant and necessary. Records for the primary purpose of the system are maintained in accordance with National Archives and Records Administration (NARA)-approved schedules N1-237-83-01, Item 11 (7), Regulatory Records (Petitions for exemptions). These records will be transferred to NARA's Federal Records Center two years from the grant or denial date. The Federal Records Center will destroy the records three years after their receipt.

System access records are maintained in accordance with NARA General Records Schedule (GRS) 3.2, Information Systems Security Records, approved January 2, 2023 and are destroyed when business use ceases.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

ASKME 2 ADD does not share information externally unless disclosure is required by law and does not use PII in any matter that is incompatible with the purpose for which it was collected.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Users can edit their AMOC up to the point of submission. After the AMOC has been submitted the user can contact the ASE to make changes to their AMOC.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure,

as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the ASKME 2 - ADD system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST. Only FAA personnel with a need to know are authorized to access the records in ASKME 2 ADD. All data in-transit is encrypted. Access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and is limited according to job function. Registration is not required to use the ASKME 2 ADD external portal; however, external users must consent to the "System Use Notice" statement before proceeding to the AMOC Requester webpage. Additionally, FAA conducts an annual cybersecurity assessment to test and validate security processes, procedures and postures of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issued ASKME 2 an authorization to operate on May 19, 2025. ASKME 2 ADD is part of the ASKME security boundaries.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA will implement additional policies and procedures as needed as they relate to the access, protection, retention, and destruction of PII. Federal

employees and contractors who work with ASKME 2 are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of ASKME 2 as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Brenda Bailey
System Owner
FAA Information Technology Solution Delivery Service Development and Sustainment Division Solutions Operations Section C

Prepared by: Michael Bjorkman, Acting FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.01.26 12:58:53 -05'00'