U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Aviation Safety (AVS)

Aviation Safety Knowledge Management Environment (ASKME 2) Compliance and Enforcement Actions (CEA)

Responsible Official

Brenda Bailey
Email: Brenda.Bailey@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Aviation Safety Knowledge Management Environment (ASKME 2) Compliance and Enforcement Actions (CEA) is managed by the FAA's Office of Aviation Safety (AVS) and operates under authorities 14 C.F.R. Part 13 §§ 13.1 – 13.29, 49 U.S.C §§ 40123 (Protection of Voluntarily Submitted Information), 49 U.S.C. §§ 46101 – 46111 (Investigations and Proceedings), and 49 U.S.C. 44701 – 44735 (Safety Regulation). 14 CFR Part 193 covers when and how the FAA protects from disclosure safety and security information submitted voluntarily to the FAA.

The AVS is the organization within the FAA that is responsible for the certification, production approval, and continued airworthiness of aircraft; and certification of pilots, mechanics, and others in aviation safety-related positions. The Aircraft Certification Service (AIR) is a department within the FAA AVS develops and administers safety standards for aircraft and related products. AIR personnel use ASKME 2 CEA to initiate and process investigations into instances of regulatory non-compliance and voluntary disclosure reports submitted by Regulated Entities (REs). REs are defined as FAA certificate holders that AIR oversees, such as type certificates and production certificates, etc. AIR personnel track and process compliance and enforcement actions in the ASKME 2 CEA application, based on the information collected through oversight or RE voluntary disclosure reports.

The FAA is publishing this Privacy Impact Assessment (PIA) for the ASKME 2 CEA in accordance with Section 208 of the E-Government Act of 2002 because the application processes Personally Identifiable Information (PII) from REs that may be members of the public. ASKME 2 CEA processes PII from both companies and individuals, which may include data such as names, addresses, and other contact information.

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 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 FAA is tasked with promptly and fully investigating and determining compliance requirement outcomes for all known or suspected violations of aircraft safety involving airport operation, manufacturing aircraft or aircraft parts, maintaining or operating aircraft, or shipping hazardous materials. These investigations are known as enforcement actions. During the investigation, violations may be identified. In addition, the FAA, through the Voluntary Disclosure Reporting Program (VDRP), receives reports of suspected violations from REs. The AIR personnel determine during the investigation if a violation occurred or if a reported violation has any merit. ASKME 2 CEA is an internal FAA, web-based application that maintains uploaded correspondence from RE's to the FAA and from the FAA to REs, which, in some instances, may contain PII such as individual names, addresses and contact information. The ASKME 2 CEA application is used to track, initiate, and process compliance and enforcement actions, as well as voluntary safety disclosures received from REs.

The ASKME 2 CEA application promotes and assures AIR compliance with statutory and regulatory requirements. AIR personnel use ASKME 2 CEA to initiate and process instances of regulatory non-compliance and voluntary disclosure reports submitted by REs. It consists of six main modules: administrative settings, voluntary disclosure reporting, action

[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).

determination, compliance actions, administrative actions, and legal actions. ASKME 2 CEA promotes AIR's safety mission by automating these components and allowing regulatory noncompliance to be more readily identified and mitigated. The ASKME 2 CEA application provides the following capabilities:

- Creates an AIR-wide database that is flexible, collects data, and consolidates common data.
- Provides a standard means for AIR personnel to initiate, track, and close compliance and enforcement actions.
- Provides a standard means for organization designation authorization holders, design approval holders, and production approval holders to disclose regulatory non-compliances through a web-based interface. The interface also allows the reporting entity to provide its corrective action plan and progress for eliminating the noncompliance issue.

FAA employees access the ASKME 2 CEA at https://ASKME 2.faa.gov/ceaui/ using their Personal Identity Verification (PIV) card to access the following modules:

Administrative Settings Module

The Administrative Settings Module is used by the ASKME 2 CEA system administrator to edit user profiles, create system announcements, manage correspondence templates, view the event log, and update frequently asked questions (FAQs). In doing so, the Administrative Settings Module collects the RE's full company/individual's name, address, and contact information.

Voluntary Disclosure Module

"Voluntary disclosures" are violations of the Federal Aviation Regulations that REs discover on their own and self-report to the FAA. REs initiate the voluntary disclosure process by submitting a letter, via mail or email, to the appropriate Aircraft Certification Office through the VDRP. Voluntary disclosure letters submitted by the RE generally include the following information: the full company/individual's name, email address, mailing address, and telephone number.

The letter also includes a brief description of the apparent noncompliance, including an estimate of the duration of time that it remained undetected, and information regarding whom, where, how, and when it was discovered; verification the noncompliance has ceased; a brief description of immediate action; a description of the Corrective Action Plan (CAP) if needed; verification of evaluation; and name of individual point of contact (POC) for the CAP.

Upon receipt and acceptance of these letters, Investigating Personnel (IP) access ASKME 2 CEA's Voluntary Disclosure Module to create the voluntary disclosure record. An IP creates a Voluntary Disclosure Report (VDR) record by selecting the office where the investigation

is conducted, the type of disclosure (informal or formal), full name of the RE, and RE's POC. If the POC information does not already exist in ASKME 2 CEA, an IP can manually enter a new POC by inputting their full name, email address, and telephone number. Once created, a VDR number is generated to track the transaction. An IP inputs the summary of noncompliance, causal analysis, and description of the CAP in open-text boxes within the module.

An IP also uploads any mailed letters received into this module. These letters contain RE names, addresses, and contact information. After uploading the letter, an IP can enter the following information: number of noncompliance, date submitted, corrective action completion date, summary of the noncompliance, summary of casual analyses, and summary of corrective action.

Action Determination Module

An IP logs into this module and selects from a series of drop-down text fields to answer questions that determine whether it is an administrative, formal or informal compliance, or legal enforcement action based on the type of noncompliance. Upon submitting the answers to these questions, ASKME CEA generates a tracking number used to track and retrieve specific actions in ASKME CEA related to an RE.[2]

Compliance Action Module

An IP accesses this module to initiate formal or informal compliance action. The IP uploads documents containing noncompliance evidence, which do not contain PII. They also upload correspondence received from the RE into this module, which generally includes the full name of the RE and the company/individual's contact information (email address, mailing address, and telephone number). FAA correspondence, which may be emails and letters about noncompliance, is also uploaded.

Administrative Action Module

IP access this module to initiate administrative actions [3]. The IP uploads documents containing evidence of noncompliance that does not contain PII. They also upload

[2] Tracking numbers are based on information collected in this module. Each is a unique identifier consisting of the office prefix, year, regional code, office code, and a four-digit sequential number.
[3] Per FAA Order 2150.3, administrative action occurs when FAA personnel reasonably and in good faith determine that compliance action will not remediate noncompliance and ensure future compliance; and legal enforcement action is not required. There are two types of administrative action: warning notices and letters of correction.

correspondence received from the RE into this module, which generally includes the RE's full name and the company/individual's contact information (email address, mailing address, and telephone number). FAA correspondence, which may be emails and letters about noncompliance, is also uploaded.

Legal Enforcement Action Module

IP access this module to record information that may potentially lead to legal action, such as civil penalties. FAA tracks potential legal enforcement actions in the Enforcement Information System (EIS) [4]. ASKME 2 CEA's legal enforcement action module is a preliminary step to entering non-compliances requiring legal enforcement to EIS. The IP uploads documents containing noncompliance evidence, which do not contain PII. They also upload correspondence received from the RE into this module, which generally includes the following information: full name of RE; company/individual's contact information (email address, mailing address and telephone number), make, model, and/or series number of aircraft, aircraft engine, aircraft propeller or part involved. FAA correspondence, which may be emails and letters about noncompliance [5], is also uploaded.

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[6], 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[7].

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

[4] The PIA for EIS is published at Enforcement Information System (EIS) & EIS Query and Browse Database (EISQB) | US Department of Transportation. FAA uses the Office of General Counsel's workload system, Case and Document Management System (CDMS), to process enforcement actions. A PIA for CDMS is in progress.
[5] These emails and letters do not contain any additional PII that was not already listed previously.
[6] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[7] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Individuals mail or email voluntary disclosure reports to AIR, and thus, no notice is provided. IPs upload documents and correspondence to ASKME 2 CEA and notice may be provided on uploaded documents that are subject to the Privacy Act. The FAA retrieves records in ASKME 2 CEA by an individual's name and other personal identifiers and protects records subject to the Privacy Act in accordance with Department's Published System of Records Notices.

Voluntary disclosure reports and correspondence uploaded into ASKME 2 CEA are covered by DOT/FAA 847, Aviation Records on Individuals, 89 FR 48956, (June 10, 2024).

User access records, are also retrieved by identifier such as full names, and are subject to DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30757.

Finally, the publication of this PIA also demonstrates DOT's commitment to providing appropriate transparency into the ASKME 2 CEA application.

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.

PII may be present in uploaded documents which individuals mail or email to ASKME 2 CEA. Individuals who wish to update or correct information stored in ASKME 2 CEA should make their requests in writing to their FAA Point of Contact, such as the principal inspector or Organizational Management Team (OMT) member.

Furthermore, under the provisions of the Privacy Act, individuals may request a search to determine if records maintained in ASKME 2 CEA pertain to them. To request a search, individuals may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

The following must be included in all requests:

- Name

- Mailing Address
- Phone Number and/or Email Address
- A description of the records sought, and if possible, the location of the record(s)

Individuals seeking a correction of records pertaining to them that are stored in ASKME 2 CEA should make their requests in writing. Requests must detail the reasons the records should be so corrected. Requests for corrections of records may be sent to:

Federal Aviation Administration

Privacy Office

800 Independence Ave. SW

Washington, DC 20591

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 CEA operates under the following authorities 14 C.F.R. Part 13 §§ 13.1 – 13.29, 49 U.S.C §§ 40123, Protection of Voluntarily Submitted Information, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings, and 49 U.S.C. 44701 – 44735 Safety Regulation. 14 CFR Part 193 covers when and how the FAA protects from disclosure safety and security information submitted voluntarily to the FAA.

The FAA's central mission is to promote safety in civil aeronautics. To achieve this mission, the agency establishes regulatory standards and requirements, found in 14 Code of Federal Regulations (C.F.R.) parts 1-199 under the statutory authority in 49 United States Code (U.S.C.) subtitle VII. Under 49 U.S.C. § 40113, the FAA Administrator has broad authority to take action the Administrator considers necessary to carry out DOT statutory responsibilities and powers relating to safety in air travel, including issuing regulations and standards, conducting investigations and issuing related orders. The authority to carry out investigations and conduct enforcement proceedings fall under 14 CFR Part 13 §§ 13.1 – 13.29, 49 U.S.C. §§ 46101 – 46111 Investigations and Proceedings, and 49 U.S.C. 44701 – 44735 Safety Regulation.

ASKME 2 CEA records are used to initiate and process instances of regulatory noncompliance discovered by AIR personnel during routine oversight activities. ASKME 2 CEA records are also used to process Voluntary Disclosure Reports submitted by REs. AIR personnel track and process compliance and enforcement actions in the ASKME 2 CEA, based on the information collected from audits, oversight or RE voluntary disclosure reports.

ASKME 2 CEA sends or receives information from the following FAA IT systems:

Aviation Safety Knowledge Management Environment – Enterprise Service (ASKME 2 ES) receives the following:

- ASKME 2 ES *User Profile Service:* receives ASKME 2 CEA users' full name, email address, telephone number, and business address to authenticate and verify the user is active in ASKME 2 ES and has an ASKME 2 CEA user role.

- ASKME 2 ES *Administration Application:* receives ASKME 2 CEA users' full name, email address, telephone number, and business address to manage user accounts, update or edit ASKME 2 CEA user information.

ASKME 2 ES: sends verification the ASKME 2 CEA user has an active profile in ASKME 2 ES and validates the ASKME 2 CEA user role.

Tableau[8]*:* receives analytic data exported via Excel file from ASKME 2 CEA that includes the number of compliance actions for a given office or RE, the full name of the RE, email address, mailing address, and telephone number. The purpose of the data exchange is to allow Tableau to generate a variety of reports and data visualization tasks relevant to ASKME 2 CEA's business needs.

Federal Aviation Administration Directory Services (FAA DS): ASKME 2 CEA receives user's name and email address from FAA DS. The information is used to validate system access and authentication of authorized FAA employees.

Enforcement Information System (EIS)[9]: ASKME 2 CEA sends EIS information that includes RE's full name, business name, mailing address, and telephone number; aircraft make, model, and/or series number; engine; propeller or part involved; date and time of violation, region of discovery, location of violation, reporting inspector's full name, investigating office, 14 CFR regulation(s) believed violated, recommended type action, recommended sanction, region, and full name and title of approving official. The purpose of the manual data entry is to process ASKME 2 CEA-initiated actions via EIS.

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.

[8] The PIA for Tableau is published at Tableau | US Department of Transportation
[9] The PIA for EIS is published at Enforcement Information System (EIS) & EIS Query and Browse Database (EISQB) | US Department of Transportation.

ASKME 2 CEA collects the minimum amount of information from REs to track regulatory noncompliance actions and VDRs. AIR personnel use ASKME 2 CEA to initiate and process regulatory noncompliance and VDRs submitted by REs.

ASKME 2 CEA maintains records in accordance with the following National Archives and Record Administration (NARA) approved General Retention Schedules (GRS). Records are maintained as follows:

Records that are uploaded are digitized are maintained in accordance with GRS 4.5, item 10, Approved June 2023, Digitizing Records . FAA maintains hard copy records of digitized records for five years to meet its business function.

Records relating to the investigation of violation of rules, regulation and orders are maintained in accordance with N1-237-92-4, Enforcement Records/DAA-0237-2021-0010 *Compliance Actions against individuals and entities*. Records are destroyed five years after regulatory compliance activity closes. Violation Tracking Records that result from a regulatory compliance action against entities are destroyed 20 years after the entity or its successor ceases to operate.

System access records are maintained in accordance with GRS 3.2, item 30, Approved January 2023, Information Systems Security Records. These records 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.

FAA limits the use of ASKME 2 CEA data to the purposes specified in Department published SORN DOT/FAA 847, Aviation Records on Individuals, 89 FR 48956, (June 10, 2024).

In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- To the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.
- To the public (including government entities, title companies, financial institutions, international organizations, and others), when permitted, information, including aircraft owner's name, address, United States Registration Number, aircraft type and legal documents related to title or financing of an aircraft.
- To law enforcement, when necessary and relevant to an FAA enforcement activity.

- To government agencies, whether Federal, State, Tribal, local or foreign, information necessary or relevant to an investigation of a violation or potential violation of law, whether civil, criminal, or regulatory, that the agency is charged with investigating or enforcing; as well as, to government agencies, whether Federal, State, or local responsible for threat detection in connection with critical infrastructure protection.

For information collected for system access, FAA limits the use of that data to the purposes specified in Department published SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30757

- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.
- To other government agencies where required by law.

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).

The FAA collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. The IP manually enters information into ASKME 2 CEA and performs a check as information is being entered. Records for compliance actions and enforcement actions require a management review. Data quality control reviews are conducted annually on a random sampling of records. Paper records are stored in a locked filing cabinet for five years and can be referenced as part of the quality control process.

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 CEA 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 CEA. All data in-transit is encrypted and access to electronic records is controlled by PIV and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessments to test and validate the system's security process, procedures and posture. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues ASKME 2 CEA an on-going authorization to operate.

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.

The DOT/FAA implements 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 CEA 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 CEA 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: Barbara Stance, 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: 2025.06.13 11:56:25 -04'00'