U.S. Department of Transportation

Office of the Chief Information Officer (OCIO)

Privacy Threshold Assessment (PTA)

Federal Aviation Administration

Office of Aviation Safety

Pilot Medical Disclosure Decision Making Survey

ABRAHAM MICAH EVANS SR

Digitally signed by ABRAHAM MICAH EVANS SR
Date: 2025.10.09 06:41:05 -04'00'

Privacy Threshold Assessment (PTA)

The Privacy Threshold Assessment (PTA) is an analytical tool used to determine the scope of privacy risk management activities that must be executed to ensure that the Department's initiatives do not create undue privacy risks for individuals.

The Privacy Threshold Assessment (PTA) is a privacy risk management tool used by the Department of Transportation (DOT) Chief Privacy Officer (CPO). The PTA determines whether a Department system[1] creates privacy risk for individuals that must be further analyzed, documented, or mitigated, and determines the need for additional privacy compliance documentation. Additional documentation can include Privacy Impact Assessments (PIAs), System of Records notices (SORNs), and Privacy Act Exemption Rules (Exemption Rules).

The majority of the Department's privacy risk emanates from its direct collection, use, storage, and sharing of Personally Identifiable Information (PII),[2] and the IT systems used to support those processes. However, privacy risk can also be created in the Department's use of paper records or other technologies. The Department may also create privacy risk for individuals through its rulemakings and information collection requirements that require other entities to collect, use, store or share PII, or deploy technologies that create privacy risk for members of the public.

To ensure that the Department appropriately identifies those activities that may create privacy risk, a PTA is required for all IT systems, technologies, proposed rulemakings, and information collections at the Department. Additionally, the PTA is used to alert other information management stakeholders of potential risks, including information security, records management and information collection management programs. It is also used by the Department's Chief Information Officer (CIO) and Associate CIO for IT Policy and Governance (Associate CIO) to support efforts to ensure compliance with other information asset requirements including, but not limited to, the Federal Records Act (FRA), the Paperwork Reduction Act (PRA), the Federal Information Security Management Act (FISMA), the Federal Information Technology Acquisition Reform Act (FITARA) and applicable Office of Management and Budget (OMB) guidance.

Each Component establishes and follows its own processes for developing, reviewing, and verifying the PTA prior to its submission to the DOT CPO. At a minimum the PTA must be reviewed by the Component business owner, information system security

[1] For the purposes of the PTA the term "system" is used throughout document but is not limited to traditional IT systems. It can and does refer to business activity and processes, IT systems, information collection, a project, program and/or technology, and proposed rulemaking as appropriate for the context of the assessment.

[2] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

manager, general counsel, records officers, and privacy officer. After the Component review is completed, the Component Privacy Office will forward the PTA to the DOT Privacy Office for final adjudication. Only PTAs watermarked "adjudicated" and electronically signed by the DOT CPO are considered final. Do NOT send the PTA directly to the DOT PO; PTAs received by the DOT CPO directly from program/business owners will not be reviewed.

If you have questions or require assistance to complete the PTA please contact your Component Privacy Officer or the DOT Privacy Office at privacy@dot.gov. Explanatory guidance for completing the PTA can be found in the PTA Development Guide found on the DOT Privacy Program website, www.dot.gov/privacy.

PROGRAM MANAGEMENT

SYSTEM name: Pilot Medical Disclosure Decision Making Survey

Cyber Security Assessment and Management (CSAM) ID: N/A

SYSTEM MANAGER CONTACT Information:

Name: **Julia Beckel**

Email: Julia.l.beckel@faa.gov

Phone Number: 405-954-1905

Is this a NEW system?

☒ **Yes** (Proceed to Section 1)

☐ **No**

☐ **Renewal**

☐ **Modification**

Is there a PREVIOUSLY ADJUDICATED PTA for this system?

☐ **Yes:**

Date:

☒ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

☐ **Information Technology and/or Information System**

Unique Investment Identifier (UII): Click here to enter text.

Cyber Security Assessment and Management (CSAM) ID:

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN):

Rulemaking Stage:

☐ **Notice of Proposed Rulemaking (NPRM)**

☐ **Supplemental NPRM (SNPRM)**:

☐ **Final Rule**:

Federal Register (FR) Notice: Click here to enter text.

☒ **Information Collection Request** (ICR)[3]

☒ **New Collection**

☐ **Approved Collection or Collection Renewal**

☐ **OMB Control Number:** The Program is working with the Paperwork Reduction Office to obtain OMB approval.

☐ **Control Number Expiration Date:**

☒ **Other:** Survey

1.2 System OVERVIEW: The Federal Aviation Administration (FAA) is developing the initial Privacy Threshold Assessment (PTA) for the Pilot Medical Disclosure Decision Making Survey. The survey will be used to conduct a research study about how pilots make decisions regarding the disclosure of health conditions to the FAA. This study aims to better understand pilot experiences, concerns, and thought processes around medical disclosure. The goal is to inform efforts to reduce unnecessary barriers and burdens in the reporting process.

The Civil Aerospace Medical Institute (CAMI) National Airspace System Safety Research Laboratory (AAM-520) is administering this survey on behalf of the Office of Aerospace Medicine (OAM) with the assistance of Cherokee Federal, a third-party contractor.

The survey will be conducted from October 2025 until October 2026. The universe of potential respondents includes 148,306 Air Transport pilots[4] represented within the aerospace medical certification database. The minimum sample required to detect an effect from the current collection is 1,950 responses. Given prior response rates of 35% for previous surveys conducted by the FAA, the FAA will sample 51,907 of the total number of Air Transport pilots.

CAMI has a contract in place with online survey development software Qualtrics to administer the survey. Cherokee will use Qualtrics to create the survey, collect survey responses, and create survey item reports. Cherokee staff will use their FAA email address to create a Qualtrics user account and log in with a username and password.

Cherokee will mail via the Postal Service and email participants to be surveyed, an invitation to participate in the survey, and provide each of them a unique

[3]See 44 USC 3501-3521; 5 CFR Part 1320

[4] Commercial, private, student, and recreational pilots are not included in the population of interest for this survey.

uniform resource locator (URL), a QR code to complete the survey online, and a system-generated password unique to each pilot in the sample pool.

The participants will include pilots who have previously participated in CAMI's research and have indicated interest in future involvement, for whom Cherokee has the names and email addresses. In addition, researchers for this study are also working closely with the Air Line Pilots Association, International (ALPA), the world's largest pilot union, which will provide email and mailing addresses of interested pilots within the union that would like to participate in the survey. The list provided by ALPA will be given directly to Cherokee to coordinate communication.

Once the participant accesses their unique Qualtrics link (whether URL or QR code), they receive the informed consent notice, which provides an overview of the study, its voluntary nature, and ability to opt out, informs them about the purposes of the study, and how FAA will use the results. The informed consent also advises the survey participant of FAA's PII processing activities, such as the de-identification of survey responses, which is designed to reduce the project's privacy risks. Each participant must accept the informed consent notice by agreeing to the statement, "By clicking 'Next', you are consenting to participate." All participants receive informed consent prior to taking the survey and must provide their consent before continuing with the survey.

The survey is designed with plans to obtain a response rate of approximately 1,950 participants. If, after a period of time, not enough responses are received, Cherokee sends out to all nonresponding participants another offer to participate. The survey will be closed once a response rate of 1,950 has been met.

After the survey is closed, Cherokee will download survey response data records to FAA-owned servers with access limited to certain Cherokee contractor staff and FAA Management. Cherokee will remove all PII from Qualtrics and exported databases after downloading is completed. The survey includes two questions

survey question.pdf

for which a text response can be included. Cherokee will review the text responses for any PII that participants may have provided and remove. The questions in the survey are designed not to collect PII; the Qualtrics survey has internal controls that limit the information that can be input into the survey. For example, fields that require numerical entries do not include alpha characters.

The question prompts are accompanied by reminders to participants not to include PII in their responses.

Additionally, Cherokee aggregates the responses into group-level results. The final survey dataset will contain only aggregated responses and no PII; this final survey dataset is then sent back to CAMI researchers for analysis to evaluate customer satisfaction and determine whether any changes are suggested from the results.

CAMI, including Cherokee, strictly adheres to ethical standards, public law, and federal policies for safeguarding the confidentiality of all participants in this survey. All data provided will be kept private in accordance with legal and regulatory requirements.

How the Survey will be Used and Maintained

The customer service opinions provided by participants aim to better understand pilot experiences, concerns, and thought processes around medical disclosure. The goal is to inform efforts to reduce unnecessary barriers and burdens in the reporting process. This information will be provided in the form of briefings and technical reports that contain only group-level aggregated and deidentified data.

Survey respondents are compensated for their participation. The survey includes a direct link to a secure website for a third-party contractor, Neese Personnel, to directly collect PII from the survey respondent to facilitate payment, including the respondent's name, mailing address, and email address. Cherokee sends an encrypted email with the survey respondent's name to Neese to verify the participant's name, and Neese facilitates payment by mailing a check to the respondent. The information Neese Personnel collects will not be shared. Neese Personnel will maintain this information for three years to meet requirements set forth by the Fair Labor Standards Act (FLSA). Neese Personnel stores any hard copy documents in locked, access-controlled cabinets. Electronic data is stored in

password- and firewall-protected systems[5]. At the end of the three-year retention period, any hard copy documents are shredded, and electronic files are deleted.

2 INFORMATION MANGEMENT

2.1 SUBJECTS of Collection

Identify the subject population(s) for whom the system collects, maintains, or disseminates PII. (Check all that apply)

☒ **Members of the public:**

☒ **Citizens or Legal Permanent Residents (LPR)**

☐ **Visitors**

☐ **Members of the DOT Federal workforce**

☒ **Members of the DOT Contract workforce**

☐ **System Does Not Collect PII.** If the system does not collect PII, proceed directly to question 2.3.

2.2 What INFORMATION ABOUT INDIVIDUALS will be collected, used, retained, or generated?

Survey Participants: *name, email address and home address.*

FAA contractors: *username and password*

2.3 Does the system RELATE to or provide information about individuals?

☒ **Yes**: It can relate to FAA contractors with Qualtric user accounts.

☐ **No**

2.4 Does the system use or collect SOCIAL SECURITY NUMBERS (SSNs)? (This includes truncated SSNs)

☐ **Yes:**

Authority:

Purpose:

[5] Neese Personnel may need to keep hard copy records for legal compliance, per its own record retention policy.

☒ **No**: The system does not use or collect SSNs, including truncated SSNs. Proceed to 2.6.

2.5 Has an SSN REDUCTION plan been established for the system?

☐ **Yes:**

☐ **No:**

2.6 Does the system collect PSEUDO-SSNs?

☐ **Yes:**

☒ **No**: The system does not collect pseudo-SSNs, including truncated SSNs.

2.7 Will information about individuals be retrieved or accessed by a UNIQUE IDENTIFIER associated with or assigned to an individual?

☐ **Yes**

Is there an existing Privacy Act System of Records notice (SORN) for the records retrieved or accessed by a unique identifier?

☒ **Yes:**

SORN*:* DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

☐ **No:**

Explanation:

Expected Publication:

☐ **Not Applicable:** Proceed to question 2.9

2.8 Has a Privacy Act EXEMPTION RULE been published in support of any Exemptions claimed in the SORN?

☐ **Yes**

Exemption Rule:

☐ **No**

Explanation:

Expected Publication:

☒ **Not Applicable**: SORN does not claim Privacy Act exemptions.

2.9 Has a PRIVACY IMPACT ASSESSMENT (PIA) been published for this system?

☐ **Yes:**

☒ **No**: Initial PTA.

☐ **Not Applicable:** The most recently adjudicated PTA indicated no PIA was required for this system.

2.10 Does the system EXCHANGE (receive and/or send) DATA from another INTERNAL (DOT) or EXTERNAL (non-DOT) system or business activity?

☒ **Yes:** Cherokee Federal Solutions, L.L.C. will receive from ALPA the email and mailing addresses of those who have agreed to participate in the survey. Since individuals are consenting to participate, no MOU is required.

Cherokee sends an encrypted email with the survey respondent's name to Neese to verify the participant's name, and Neese facilitates payment by mailing a check to the respondent.

☐ **No**

2.11 Does the system have a National Archives and Records Administration (NARA)-approved RECORDS DISPOSITION schedule for system records?

☒ **Yes:**

Schedule Identifier: *National Archives and Records Administration, General Records Schedule 3.2, approved January 2023*, Information System Security Records, item 30 System access records.

Schedule Summary: Destroy when business use ceases.

Schedule Identifier: *Federal Aviation Administration, Survey Study Record Schedule.* DAA-0237-2019-0004

Schedule Summary:

- Item 0001: Survey Questionnaire/Responses. Cutoff when survey study is complete. Destroy 3 years after cutoff.
- Item 0002: Survey Study Findings. Cutoff when survey study is complete. Destroy 25 years after cutoff.
- Item 0003: Survey Reports. Cutoff when survey study is complete. Destroy 25 years after cutoff.

☐ **In Progress**

☐ **No:**

3 SYSTEM LIFECYCLE

The systems development life cycle (SDLC) is a process for planning, creating, testing, and deploying an information system. Privacy risk can change depending on where a system is in its lifecycle.

3.1 Was this system IN PLACE in an ELECTRONIC FORMAT prior to 2002?

The E-Government Act of 2002 (EGov) establishes criteria for the types of systems that require additional privacy considerations. It applies to systems established in 2002 or later, or existing systems that were modified after 2002.

☐ **Yes**:

☐**No**

☒**Not Applicable**: System is not currently an electronic system. Proceed to Section 4.

3.2 Has the system been MODIFIED in any way since 2002?

☐ **Yes**: The system has been modified since 2002.

☐ **Maintenance.**

☐ **Security.**

☐ **Changes Creating Privacy Risk**:

☐ **Other**:

☐ **No**: The system has not been modified in any way since 2002.

3.3 Is the system a CONTRACTOR-owned or -managed system?

☐ **Yes**: The system is owned or managed under contract.

Contract Number:

Contractor:

☐ **No**: The system is owned and managed by Federal employees.

3.4 Has a system Security Risk CATEGORIZATION been completed?

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The OA Privacy Officer should be engaged in the risk determination process and take data types into account.

☐ **Yes**: A risk categorization has been completed.

Based on the risk level definitions and classifications provided above, indicate the information categorization determinations for each of the following:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Based on the risk level definitions and classifications provided above, indicate the information system categorization determinations for each of the following:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

☐ **No:** A risk categorization has not been completed. Provide date of anticipated completion. Click here to enter text.

3.5 Has the system been issued an AUTHORITY TO OPERATE?

☐ **Yes:**

Date of Initial Authority to Operate (ATO):

Anticipated Date of Updated ATO:

☐ **No:**

☐ **Not Applicable**: System is not covered by the Federal Information Security Act (FISMA).

4 COMPONENT PRIVACY OFFICER ANALYSIS

The Component Privacy Officer (PO) is responsible for ensuring that the PTA is as complete and accurate as possible before submitting to the DOT Privacy Office for review and adjudication.

COMPONENT PRIVACY OFFICER CONTACT Information

Name: Essie L. Bell

Email: essie.bell@faa.gov

Phone Number: 202-267-6034

COMPONENT PRIVACY OFFICER Analysis

See below

5 COMPONENT REVIEW

Prior to submitting the PTA for adjudication, it is critical that the oversight offices within the Component have reviewed the PTA for completeness, comprehension and accuracy.

Component Reviewer	Name	Review Date
Business Owner	Julia Beckel	*8/21/2025*
General Counsel	*Christopher Andrews*	*9/15/2025*
Information System Security Manager (ISSM)	Click here to enter text.	
Privacy Officer	*Essie L. Bell*	*8/21/2025*
Records Officer	*Carly Docca*	*8/20/2025*

Table 1 - Individuals who have reviewed the PTA and attest to its completeness, comprehension and accuracy.

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
AP-1	Authority to Collect	1.2 - Overview		X		14 CFR part 47, 107, 336/349 The Program is working with the Paperwork Reduction Office to obtain OMB approval.	Create AP-1 POA&M **Issue:** Instrument of collection requires PRA approval. **Requirement:** Submit instrument to OMB for approval before collection. **Timeline:** before collection. Note: PRA Package must be approved before collection.
AP-2	Purpose Specification	1.2 - Overview	X			Purpose defined.	Concur
AR-1	Governance and Privacy Program	Common Control	X			Addressed by DOT CPO.	Concur
AR-2	Privacy Impact and Risk Assessment	Program Management		X		The name, mail, and email address are used to disseminate the survey. The survey questions are not written to collect PII; however, response questions are reviewed, and all PII is	Create AR-2 POA&M **Issue:** ICR is collecting PII from members of the public. **Requirement:** Develop PIA.

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
						removed if inserted in the two questions that have open-text comments. The contact information is used to facilitate an FAA business process, so no PIA is required.	**Timeline:** 180 days. Note: per E-GOVT Act of 2002. The E-Government Act requires agencies to conduct a PIA before: developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
AR-3	Privacy Requirements for Contractors and Service Providers	3.3 - Contractor System		X		The system is owned and managed by Federal employees.	Create AR-3 POA&M **Issue:** It is unclear if the contract has the proper clauses. **Requirement:** Review contract to ensure the appropriate clauses are present. **Timeline**: 180 days. Note: PTA States "CAMI has a contract in place with online survey development software Qualtrics to administer the survey. Cherokee will use Qualtrics to create the survey, collect survey responses, and create survey item reports."
AR-4	Privacy Monitoring and Auditing	Common Control	X			Addressed by DOT CPO.	Concur
AR-5	Privacy Awareness and Training	Common Control	X			Addressed by DOT CPO.	Concur

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
AR-6	Privacy Reporting	Common Control	X			Addressed by DOT CPO.	Concur
AR-7	Privacy-Enhanced System Design and Development	2.5 - SSN Reduction			X	SSN not collected. The business owner is responsible for ensuring DOT Privacy Risk Management Policy and the FIPPs are applied to all data holdings and systems.	Concur
AR-8	Accounting of Disclosures	2.7 - SORN			X	Substantive records are not retrieved by an identifier linked to an individual and the records are not about individuals and are therefore not protected by the Privacy Act. Records created for account creation, logging, auditing, etc., are covered by DOT/ALL-13.	Concur
DI-1	Data Quality	1.2 - System Overview	X			Data quality is determined by OA information system owners.	Concur

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
DI-2	Data Integrity and Data Integrity Board	3.4 - Security Risk Categorization			X	Activity does not constitute sharing covered by the CMA.	Concur
DM-1	Minimization of PII	2.2 – Information About Individuals	X			Collection of PII commensurate with purpose of the system. Not a Privacy Act System of Records. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13..	Concur
DM-2	Data Retention and Disposal	2.11 - Records Disposition Schedule	X			A retention schedule is in place.	Concur
DM-3	Minimization of PII Used in Testing, Training, and Research	2.2 – Information About Individuals	X			CAMI uses de-identification and other techniques to minimize the PII processed through this survey project. System not used for testing, training, research.	Concur
IP-1	Consent	2.7 - SORN			X	Control is N/A. Substantive records are not retrieved by an identifier linked to an individual and the records are	Satisfied - Consent mechanism established with Cherokee,

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
						not about individuals and are therefore not protected by the Privacy Act. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.	information is collected directly from individuals.
IP-2	Individual Access	2.8 – Exemption Rule			X	Control is N/A. Substantive records are not retrieved by an identifier linked to an individual and the records are not about individuals and are therefore not protected by the Privacy Act. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.	Concur
IP-3	Redress	2.7 - SORN			X	Control is N/A. Substantive records are not retrieved by an identifier linked to an individual and the records are not about individuals and are therefore not protected by the Privacy Act.	Concur

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
						Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.	
IP-4	Complaint Management	Common Control	X			Addressed by DOT CPO.	Concur
SE-1	Inventory of PII	Common Control	X			This is a survey and is not a privacy-sensitive system. It is not an IT system under FISMA, so there will be no CSAM ID or risk acceptance package for the survey. A copy of the PTA will be maintained in the FAA Privacy compliance tracker, and findings will be tracked by FAA Privacy.	Concur
SE-2	Privacy Incident Response	Common Control	X			Addressed by DOT CPO.	Concur
TR-1	Privacy Notice	2.7 - SORN			X	Control is N/A. Substantive records are not retrieved by an identifier linked to an individual and the records are not about individuals and are therefore not protected by the Privacy Act.	Concur

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
						Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.	
TR-2	System of Records Notices and Privacy Act Statements	2.7 - SORN			X	Control is N/A. Substantive records are not retrieved by an identifier linked to an individual and the records are not about individuals and are therefore not protected by the Privacy Act. Records created for the purposes of account creation, logging, auditing, etc. are covered by DOT/ALL-13.	Concur
TR-3	Dissemination of Privacy Program Information	Common Control	X			Addressed by DOT CPO.	Concur
UL-1	Internal Use	2.10 - Internal and External Use			X	Information not authorized for disclosure beyond FAA/FAA-contractors.	Concur

Control #	Control Name	Primary PTA Question	Satisfied	Other than Satisfied	N/A	Component PO Assessment	DOT CPO Assessment
UL-2	Information Sharing with Third Parties	2.10 - Internal and External Use		X		Cherokee Federal Solutions, L.L.C. will receive from ALPA the email and mailing addresses of those who have agreed to participate in the survey. No MOU is required. Cherokee sends an encrypted email with the survey respondent's name to Neese to verify the participant's name, and Neese facilitates payment by mailing a check to the respondent.	Create UL-2 POAM **Issue:** ALPA and Cherokee shares PII without and MOU. **Requirement:** Develop MOU. **Timeline:** 180 days.