U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Designee Management System (DMS)

Responsible Official

Linda Navarro
Email: linda.navarro@faa.gov
Phone Number: 405-954-9808

Reviewing Official

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

July 6, 2022

Executive Summary

Title 14 Code of Federal Regulations Part 183 is the statutory authority that describes the requirements for designating private persons to act as representatives of the Administrator in examining, inspecting, and testing persons and aircraft for the purpose of issuing airman, operating, and aircraft certificates. These private persons are called designees and their function is vital to enhancing the Federal Aviation Administration's (FAA) public service role and improving overall safety in the National Airspace System (NAS). The FAA appoints designees to provide airmen and aircraft certifications, conduct inspections, and other services to the public in accordance with FAA policy, guidance, and regulations on behalf of the FAA Administrator.

Based on a recommendation from the Government Accountability Office (audit GAO-05-40) stating there should be one comprehensive system to manage all designees across Aviation Safety, the FAA developed the Designee Management System (DMS). The DMS standardizes the management lifecycle process of designees and provides the official repository of applicants along with oversight of appointed designees.

The FAA is publishing this Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 because DMS collects and maintains personally identifiable information (PII) from applicants trying to become designees and appointed designees. In addition, designees may enter information on airmen who are seeking to qualify for a certification.

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]

[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).

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 Federal Aviation Act of 1958, as amended, gives the FAA the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

DMS is a web-based application located at https://designee.faa.gov and it is used to standardize the management lifecycle process and oversight of designees and is the official repository of applicants along with oversight of appointed designees. Designees are representatives of the FAA who are authorized to perform certification-related tasks (i.e., conduct examinations, testing, inspections, and issue certificates) on behalf of the FAA Administrator. The FAA has limited resources to perform all certification activities; therefore, it is necessary to appoint designees to carry out these tasks. FAA's categories of designees include the following:

- AIR/Designated Manufacturing Inspection Representative (DMIR)
- Designated Airworthiness Representative – Manufacturing (DAR-F)
- AAM/Aviation Medical Examiner (AME)
- FS/Designated Airworthiness Representative – Maintenance (DAR-T)
- Designated Pilot Examiner (DPE)
- Designated Parachute Rigger Examiner (DPRE)
- Designated Mechanic Examiner (DME)
- Specialty Aircraft Examiner (SAE)
- Administrative Pilot Examiner (Admin PE)
- Aircrew Program Designee (APD)
- Training Center Evaluator (TCE)
- Designated Aircraft Dispatch Examiner (DADE)
- Designated Engineering Representatives (DERs)

Appointed designees log into DMS by entering their username and password. Applicants seeking appointment as a designee navigate to https://designee.faa.gov to register and manually enter the following information:

- Name
- Email address
- Username
- Password
- Select a security question and provide an answer (could include PII)

After entering the information, the applicant immediately receives an auto-generated email notifying them that their registration is complete. To proceed with the application to become a designee, the applicant logs into DMS by entering their username and password. The application process in DMS is essentially the same for all designation types. The applicant initiates an application by selecting the type of designation(s) of interest and then manually enters the following information to create their profile:

- Name
- Suffix
- Date of Birth
- Airman Certification Number
- Gender
- Country of Citizenship
- Contact Phone Number
- Upload photo (optional)
- Personal Address

- Designee's Mailing Address (same as personal or business address)
- FAA Tracking Number (FTN)[2]
- Name(s) and phone number(s) of individuals listed on their application to serve as the applicant's character and/or technical references
- Employer name/employer point of contact[3]
- Designation Type and Location
- Medical License Number/National Provider Identifier[4]
- Upload of supporting documents that may include:[5]

    - Professional resume detail education and work experience
    - Training and Certification Information
    - License(s) and Certificate(s) Information
    - Character and/or technical reference name(s) and phone number(s)
    - Applicant's company representative(s) name(s) and phone number(s)

In addition, applicants answer "Yes/No" background questions pertaining to military service, prior or current legal action, felony convictions, probation, imprisonment, revocation of airmen certificate licensure, and fluency in English. From a dropdown menu, applicants select the FAA Office for which they are applying. The applicant digitally signs the application within DMS using their password to submit the application. They receive an auto-generated email from DMS describing if their submission was successful and whether they have met the minimum qualification requirements to become a designee. For applicant that do not meet the qualification requirements, the email advises them to review FAA Order 8000-95, Designee Management Policy, for qualification requirements. If an applicant feels they meet the qualification, they can check their answers and resubmit their application.

For applicants that have met the minimum qualification requirements, their request to become a designee is determined by an Evaluation Panel consisting of FAA employees and the review process occurs outside of DMS. However, once a determination is made, a specialist enters the results into DMS. Once appointed to designee status, DMS generates a Certificate Letter of Authority (CLOA) that include the authorizations granted, any limitations, and the Designation Certificate that includes the designee's name, type of designation issued, designation identification number and effective date in which the

[2] The FTN is only required if the applicant is applying for any of the following designee categories: DAR-T/DME/DPRE/DPE/SAE/Admin PE/TCE/APD/DADE
[3] The employer's name and point of contact are only required if the applicant is applying for any of the following designee categories: TCE/APD/DADE
[4] The Medical License Number/National Provider Identifier is only required if the applicant is applying for AME.
[5] Documents uploaded are dependent on the type of certification the applicant is applying for.

designee can access DMS to view and download a copy.

Designee Activities

Once appointed, some designees carry out testing on new and existing airmen to ensure they meet the requirements for the certificates they are seeking. In doing so, the airmen reach out to the designee and request the designee to perform the testing for the certification they are seeking. If an airman has an application in the Integrated Airman Certification and Rating Application (IACRA), the designee enters the airmen's FTN into the DMS activity report, and the airmen's name, address, phone, email address, and airman certificate number is auto populated with information from IACRA[6]. If the airman does not have an application in IACRA, the airmen provide the designee their name, address, phone, email address, airman certificate number and FTN and the designee enters that information into the DMS activity report. Once the test is complete, IACRA sends DMS the test date, test location, success or failure data and the aircraft used, and the designee enters the results in the DMS activity report. The information is used to track activities of the designee.

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.

[6] This access does not give the designee access to all the airman's records in the FAA.
[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

The DMS collects the name, email address, username, password, and answer to the security question, which could contain additional PII when the designee registers for an account. In addition, DMS collects the applicant's name, suffix, date of birth, airman certification number, gender, country of citizenship, phone number, email address, photo (optional), designee's mailing address (same as personal or business address), and FTN of applicants seeking to become designees. See PIA Overview Section for the complete list of PII. DMS presents applicants with a Privacy Act Statement that provides notice of the authority, purpose, routine information sharing, and the voluntary nature and consequences associated with an individual's choice to provide, or not provide, the requested information. DMS also presents applicants with a Paperwork Reduction Act (PRA) Statement that includes the Office of Management (OMB) collection number, OMB number 2120-0033.

The FAA retrieves system access records in DMS by name and other identifiers and protects Privacy Act records in accordance with Department published System of Records Notice (SORN) DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757. The applicant's information is also retrieval by name and other identifier and protected in accordance with FAA published SORN DOT/FAA 830 - Representatives of the Administrator[9].

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency about its privacy practices to those who use DMS.

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.

Registered users voluntarily provide their name, email address, username, password, and answer to the security question that could contain additional PII for account registration. Applicants can navigate https://designee.faa.gov at any time to update this information. Additionally, an applicant seeking to become a designee provides information and can change their information, discussed in the Overview section of the PIA, prior to the selection process.

Under the provisions of the Privacy Act of 1974, individuals may request searches to determine if any records pertain to them, or contest information about themselves.

[9] The DOT/FAA 830 SORN is in the process of being updated and currently with DOT Privacy for review and submission to Office of Budget and Management for approval. The finalized SORN will be published at https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices

Individuals may update their information directly through DMS. If access is no longer active, individuals may submit their requests, in writing, detailing the reasons for the corrections to the following address:

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

Included in the request must be the following:

- Name
- Mailing address
- Phone number or email address
- A description of the records
- Location of the records (if applicable)

Contesting record procedures:

Individuals wanting to contest information about themselves that is contained in DMS should make their requests in writing, detailing the reasons for why their records should be corrected, to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (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. Ex. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

Title 14 Code of Federal Regulations Part 183 is the statutory authority that describes the requirements for designating private persons to act as representatives of the Administrator in examining, inspecting, and testing persons and aircraft for the purpose of issuing airman, operating, and aircraft certificates.

DMS collects the designee's name, email address, username and password, and responses to security question(s) to create a user account and profile. DMS also collects the designee's name, date of birth, gender, country or citizenship, phone number, email

address, mailing address, business contact information, license or certification information, education, training and certification information, applicant's character/technical reference name(s) and phone number(s) as part of the application process to become a designee.

Airmen that are seeking to obtain a certification, may provide their name, address, phone, email, airmen certification number and FTN and the information is entered into DMS by the designee, and it used to facilitate testing for the certification that the designee is seeking.

DMS share information with the following internal systems:

National Automated Conformity Inspection Process (NACIP) receives the designee's names, designation identification number, phone number and type of designation for the purpose of verifying the designee has an active designation identification number.

Medical Support System (MSS) receives the designee's designation identification numbers and the status of the designees and allows the MSS to identify if a medical exam needs to be performed on a designee.

Integrated Airmen Certification and Rating Application (IACRA) provides DMS the airmen's name, address, phone, email address, and airman certificate number. IACRA receives the airman's name and application identification numbers to allow IACRA to send practical test information to DMS. The information that IACRA sends to DMS includes test type, test date, test location, success or failure data and the aircraft used. The information populates the DMS activity report and is used to track progress and activities of the designee.

Safety Assurance System (SAS) receives the designee's name, designation identification number, designee type and certification expiration date. The information is used to provide workload and resourcing.

Enhanced Flight Standards Automation System (eFSAS) receives the designee's name, designation identification number, designee type and status and the information is used to calculate pay grade. In addition, designees' name, email address, phone and location are searchable at https://designee.faa.gov to perform specific functions. Results from the search will populate a list of designees meeting the specified criteria and display designees' name, address, city, state, zip code, phone number, country, designee type, and office name.

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.

DMS collects the minimum amount of PII necessary to standardize the management lifecycle process and oversight of designees. To encourage data minimization, FAA provides a data sheet to designee applicants in the application process to explain what FAA needs. In addition, designee applications are reviewed when a need for a designee is required.

The FAA has submitted a new records retention and disposition schedule DAA-0237-2020-0013 to the National Archives and Records Administration (NARA) in which it proposes to maintain Designee Case File records for 25 years following the Designee's inactive status. The FAA will retain records in this system of records as permanent records until it receives an approval of record disposition authority from NARA.

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.

DMS does not share information with external systems. The sharing of user registration information in the DMS is conducted in accordance with DOT/ALL 13- Internet/Intranet Activity and Access Records. 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 provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems;
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;
- 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; and
- To other government agencies where required by law.

DMS share applicant seeking/or assign designees in accordance with DOT/FAA 830 - Representatives of the Administrator which permits the sharing of this information. 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:

- Provide the public with the names and addresses of certain categories of representatives who may provide service to them.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses" (available at http://www.transportation.gov/privacy).

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).

Applicants are responsible for ensuring the accuracy of their information and can access DMS to edit their profile information (contact information, personal and mailing addresses) as needed. In addition, they can make changes to their application, as needed, prior to its submission. The DMS also has an annual requirement for applicants to verify/update their application information, while appointed designees also have the same annual requirement to retain eligibility for designee status for the following year.

In addition, FAA employees monitor designee status and update a designee's authorizations if the designee has been suspended or terminated. The DMS employs various workflows to update these statuses.

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 DMS protects PII against loss, unauthorized access, or compromise with reasonable administrative, technical, and physical security safeguards. Users authenticate with their FAA domain credentials using their PIV card. Internal access to DMS is validated against Active Directory, which sends the user's name to the DMS via Integrated Windows Authentication. Applicants and FAA Designees access DMS via their username and password.

Access DMS is granted on a "need to know" basis. The DMS employs role-based access, wherein the different user roles have differing levels of access or capability. For example, a general user can only perform limited functions, where as a Managing Specialist role has full access within DMS to manage designees.

Physical security includes physical access and environmental controls in the controlled server center within a secure facility (MMAC) that houses DMS. Physical access is limited to designated personnel through photo badges, building key cards, and room-access keypads.

Training is required for FAA users depending upon their roles and responsibilities. All FAA employees and contractor personnel must complete privacy and security training and agree to the Rules of Behavior (ROBs), which emphasize privacy protective practices.

FAA incorporates 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020.

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 FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division, is responsible for governance and administration of FAA Order 1370-121B, *FAA Information Security and Privacy Program and Policy*. FAA Order 1370-121B implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-3470, the Federal Information Security Management Act (FISMA), Department of Transportation (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, additional policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT Privacy Office and the FAA Security Compliance Division (AIS-200) will conduct periodic privacy compliance reviews of DMS in accordance with the requirements of OMB Circular A-130.

Responsible Official

Linda Navarro
System Owner
Program Manager, Aviation Data Systems Branch

Approval and Signature

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer