U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Designee Registration System (DRS)

Responsible Official

Trey McClure
System Owner
9-AMC-Designee-Questions-Comments-Concerns@faa.gov
(405) 954-9510

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2018.10.16 11:27:18 -04'00'

Executive Summary

Under Title 49 of the United States Code § 44702, Congress gave the Federal Aviation Administration (FAA) the ability to delegate to qualified members of the public the authority to certify aircraft and people on behalf of the FAA Administrator. These qualified members of the public are called Designees. Designees have the authority to act on the behalf of the FAA when certifying aircraft and people to make examinations, test, inspect, and issue certificates. The FAA is responsible for the oversight and management of Designees.

To qualify Designees, the FAA developed the Designee Registration System (DRS) for the primary purpose of managing Designee required training. DRS is a training management web-based system that allows all members of the public to create DRS user profiles, select courses, pay for courses via Pay.gov, complete courses via the FAA's Blackboard system, and allows the FAA to track and manage courses. Users of DRS are individuals who are seeking to qualify as Designees, and Designees who take recurrent and specialized training. All DRS users are collectively known as Students. To create the profile to use the DRS system, individuals must identify their category of designee/designee applicant.

Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates PII. The FAA is conducting this PIA, because DRS collects and maintains Students' Personally Identifiable Information (PII) when they create a DRS user profile.

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;*

[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).

- *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

As a matter of public policy, the Designee's function is vital to enhancing the Federal Aviation Administration (FAA) public service role and improving overall safety of the national airspace. Given the agency's limited resources, using Designees for routine certification tasks allows the FAA to focus its resources on critical safety certification issues and new technologies. Designees are not FAA employees or contractors, but rather members of the public, who are subject matter experts regarding the FAA's certification regulations and requirements.

The Designee Registration System (DRS) is a web-based learning management system operated by the FAA's Office of Aviation Safety, Flight Standards Service. The mission of the Flight Standards Service is to promote safe air transportation by setting the standards for certification and oversight of airmen, air operators, air agencies, and Designees. Flight Standards Service developed DRS for the primary purpose of ensuring that all persons who seek Designee status, or maintain Designee status, take the required training necessary for them to demonstrate that they are knowledgeable about relevant FAA certification policy, guidance, and regulations.[2] Users of DRS are individuals who are seeking to qualify as Designees, and Designees who take recurrent and specialized training, All DRS users are collectively known as "Students" and will be referred to as such for the remainder of this PIA.

All DRS courses fall under the following three training categories: initial, recurrent, and specialized.[3] While all Students can access all three types of training, regulations require Designees to complete applicable types of training pertinent to their Designee status. Completion of initial training is a requirement for those Students seeking Designee appointment, and recurrent training is required to maintain their status. Completion of specialized training permits Designees to achieve higher levels of expertise. For example, Designees who conduct medical examinations of people must complete Aviation Medical Examiner specialized training. Specialized training includes topics not normally covered in the initial or recurrent training, and typically covers areas where specialized experience and authority are required.

This PIA will discuss in further detail below how DRS allows Students to create DRS user profiles, select courses, pay for courses via Pay.gov, complete enrolled courses via FAA's Blackboard system, and allows the FAA to track and manage courses.

To create a user profile**,** Students manually enter the below information into a web form on the public-facing FAA DRS website (https://av-info.faa.gov/DsgReg/userprofilecreate.aspx).

[2] *See* Designation Authority: Title 14 of the Code of Federal Regulations (14 CFR) Part 183, Representatives of the Administrator, prescribes the requirements for designating private individuals to act as representatives of the Administrator.

[3] *See,* Order 8000.95, Designee Management Policy, Chapter 7, Section 3 (June 30, 2017).

- **Mandatory Fields:**
  - Username
  - Password
  - First Name
  - Last Name
  - Daytime Phone Number
  - Street
  - City
  - State/Province/Region
  - Country
  - Zip/Postal Code
  - Primary Email Address
- **Additional Optional Fields:**
  - Middle Initial
  - Jr./Sr./III/etc.
  - Secondary Email Address
  - Company Name
  - Supervisor Name
  - Supervisor Email

When a Student creates a user profile, the system automatically generates a unique five-digit DRS tracking Identification Number (DRS tracking ID), which is linked to each Student. Students may update their user profile information or change their password at any time. Once a user profile is created, Students may use the system to select courses from the DRS course catalogue available at https://av-info.faa.gov/DsgReg/sections.aspx. Any Student with a DRS user profile may enroll, make payment, and take any DRS course regardless of their Designee status.

To enroll and pay for a course, a Student selects the course they would like to take from the course catalog, and the system automatically transfers them to the Department of Treasury's Pay.gov website to make payment. Though the Student only sees the course amount, the system transmits to Pay.gov the other information needed to support the transaction. This information is sent encrypted, and includes the following: the DRS tracking ID; the Pay.gov Agency ID (which indicates this is an FAA transaction); the Pay.gov application name and Pay.gov form ID, which identify the name and number of the form. DRS provides this information to Pay.gov to identify which Student is making a payment, to identify that the payment is being processed on behalf of the FAA, and the payment web-form information necessary to process the payment.

After this information, has been transmitted to Pay.gov, Students complete their payment for an enrolled course by submitting their billing information (e.g., name and address, and credit card or checking account information). Once a Student successfully completes their Pay.gov transaction, Pay.gov electronically transmits back to DRS the DRS tracking ID to relate that transaction to a specific Student, and a Pay.gov tracking ID, which is an automatically generated confirmation number that confirms successful payment. The Department of Treasury manages all

payment information and none of this payment information, such as credit card number, checking account number etc., is shared between Pay.gov[4] and DRS.

After successful payment is tendered at Pay.gov, Students are automatically returned to their DRS enrollments webpage, where they can directly navigate to Blackboard, a separate FAA system, to take their online courses. DRS provides Students with a single sign-on to Blackboard, which eliminates the need for Students to sign into two separate systems. Students transferred to Blackboard can either create a new Blackboard account or access their existing account. To create a new Blackboard account, DRS electronically transmits the necessary encrypted information, including full name and email address to Blackboard. Blackboard checks the email address to verify whether that Student has an existing Blackboard account. If so, that account will be accessed; if not, Blackboard creates a new Student account.

Once the Blackboard account is either accessed or created, the Student may then enroll in their courses within Blackboard. To accomplish this, DRS electronically transmits to Blackboard in encrypted form, the following Student information: enrollment role (S for Student); course owner Role (e.g., Designee, Air Students, Airports, etc.) and Blackboard course ID (the catalogue number for the course). After the Student is successfully enrolled in a course, Blackboard electronically transmits back to DRS an enrollment ID, a system-generated confirmation number for enrollment. This serves as confirmation that a Student is enrolled in an online course via Blackboard and now has access to complete that specific course.

Finally, when a Student completes a course on Blackboard, they are automatically transferred back to their DRS enrollments webpage to view their Blackboard grade and course completion. DRS electronically transmits all Students' grades from Blackboard per course ID in encrypted form, and displays them on Students' enrollments webpage. Students may view their grades and course completions at their DRS enrollments webpage.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template 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[5], 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[6].

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

[4] See the Pay.gov PIA located at https://fiscal.treasury.gov/fsreports/rpt/fspia/paygov_pia.pdf for more information on how the Department of Treasury treats individual information collected or maintained through these payment procedures.

[5] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf.

[6] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf.

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.

The FAA deploys the following techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains PII within DRS. DRS maintains records on Students which are retrievable by their name, email address, and all other DRS user profile PII listed above. The Department of Transportation (DOT) has published a Privacy Act System of Records Notice (SORN), DOT/FAA 830, *Representatives of the Administrator*, April 11, 2000 65 FR 19525, to provide notice to the public of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about an individual that may be collected.

A Privacy Act statement discussing the privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of PII is available on the DRS user profile web form.

This PIA further demonstrates DOT's commitment to provide appropriate transparency.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

All information within the DRS user profile web form is voluntarily collected from the Students, so they are active, consenting participants in the decision-making process regarding the collection of their PII. Once a Student has created a user profile, they may always go back at any time to update their information. Students may contact the FAA directly to correct their PII at 9-AMC-Designee-Questions-Comments-Concerns@faa.gov.

Additionally, under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington, DC 20591

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records.

Contesting record procedures: Individuals wanting to contest information about them that is contained in this system should make their request in writing, detailing the reasons for why their records should be corrected and addressing their letter to the following address:

Federal Aviation Administration
Privacy Office

800 Independence Avenue (Ave), SW
Washington, DC 20591

Additional information about the Department's privacy program may be found at www.transportation.gov/privacy. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

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 its collects, uses, maintains, or disseminates PII.

DRS uses of Students' information are consistent with the purposes for which it is collected, as described in DOT/FAA 830, *Representatives of the Administrator,* April 11, 2000 65 FR 19525. DRS records are required to support applications for and issuance of authorizations to be Representatives of the Administrator. They are used to identify and maintain a list of applicants for future appointment, as necessary, and to record validation and approval of new designees. Additionally, they are used to promote the standardization of designees by tracking training, accomplishments, and the limitations of current designees.

The following statutes authorize the FAA's collection and use:

- *Designation of a Designee Authorization:* Title 49 of the United States Code § 44702 empowers the Administrator to "...delegate to a qualified private person, or to an employee under the supervision of that person, a matter related to the examination, testing, and inspection necessary to issue a certificate under this chapter; and issuing the certificate."
- *Designation Authority:* Title 14 of the Code of Federal Regulations Part 183, Representatives of the Administrator, prescribes the requirements for designating private individuals to act as representatives of the Administrator.
- *Designee Authority to Act on Behalf of FAA Administrator:* Title 14 CFR Part 61, Certification: Pilots, Flight Instructors, and Ground Instructors, and 14 CFR Part 142, Training Centers, provides for individuals authorized by the Administrator to conduct functions for the initial competency validation and continued qualification.

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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The PII data elements such as name and contact information collected by the FAA are the minimum necessary to enable Students to create user profiles in DRS and complete training. Students are not obligated to provide information that is not required to create a DRS user profile. Additionally, DRS does not collect Students' payment information. Pay.gov collects and maintains Students' payment information and is managed by the Department of Treasury.

DRS gives the FAA the ability to merge duplicate Student accounts to eliminate redundant and unnecessary Student information. By eliminating unnecessary Student accounts and information, the FAA avoids having to sift through

multiple accounts to identify a Student, and eliminates superfluous Student information to only what is necessary for a Student to establish a unique DRS account.

The DRS tracking ID, Pay.gov tracking ID, and enrollment ID are numeric, automated shorthand references to the pertinent information, and permit the transactions between DRS and its two interfacing systems, Pay.gov and Blackboard, to occur without transmitting the details of Student name, payment, and contact information. The DRS tracking ID is a DRS-generated five-digit number used to identify a Student. The Pay.gov tracking ID is a Pay.gov-generated number that serves as proof of a Student having made a successful payment. An enrollment ID is a Blackboard-generated number used to confirm that a Student is enrolled in a Blackboard course. These tracking IDs are all system- generated numbers that are not linked or linkable to a Student outside of DRS, Pay.gov, and Blackboard. The use of these tracking IDs serves as a method for DRS to identify which Students have made successful payments via Pay.gov and completed courses via Blackboard, without having to share and use any of the DRS user profile information or more sensitive information (e.g., credit card number, checking account number, etc.).

Students' information is retained and disposed of in accordance with NARA approved retention schedule, II-NNA-1102, Designee Case Files (excluding Designated Medical Examiners). All Students' records, including their training reports, course enrollments, and their user profile, are destroyed 5 years after the designation becomes inactive.

Use Limitation

DOT shall limit the scope of its PII used 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.

The sharing of Student PII is conducted in accordance with DOT/FAA 830, Representatives of the Administrator, April 11, 2000 65 FR 19525. In addition to other disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:

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

The Department has also published 14 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 July 20, 2012, 77 FR 42796, under ''Prefatory Statement of General Routine Uses'' (available at http://www.transportation.gov/privacy/privacyactnotices).

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).

Automating the data exchange between DRS and Blackboard ensures data integrity by avoiding human error. Students provide their DRS user profile information and review information as entered for accuracy. Once a Student creates a DRS user profile, they may go back to their DRS user profile at any time to update their information.

Students may also contact the FAA directly to correct their PII at 9-AMC-Designee-Questions-Comments-Concerns@faa.gov.

Security

DOT shall implement administrative, technical, and physical measures 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

DRS implements administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Specifically, DRS takes the following steps to safeguard PII: identification and authentication, physical security, roles and permissions, and encryption. First, DRS uniquely identifies and authenticates users based on username and password. Users are authenticated through use of unique passwords. Second, physical access to the DRS servers is restricted to authorized personnel only. Internal FAA users request access from Administrators at the organizational level via email during the initial account creation. Once an Administrator grants access, internal FAA users use a username and password to access DRS. Third, DRS manages access to information through FAA user roles. FAA Users receive the least privileges possible to perform their job duties through the user roles. Fourth, DRS securely transmits Student information using third party authentication services, which protect the data using Hypertext Transfer Protocol (HTTP) encrypted by Transport Layer Security/Secure Sockets Layer (SSL). The DRS user profile webpage, where a Student would access to create their account, uses SSL to establish an encrypted link between a Student's web browser and DRS. Additionally, Student information maintained in DRS is encrypted. DRS was granted a three-year Authority to Operate (ATO) on August 16, 2017.

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 1370.121 implements the various privacy requirements based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347,) the FISMA, DOT privacy regulations, Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource and other mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors are given clear guidance in their duties as related to collecting, using, and processing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Order 1370.121. The FAA will conduct periodic privacy compliance reviews of the DRS as related to the requirements of OMB Circular A-130.

Responsible Official

Trey McClure
System Owner
9-AMC-Designee-Questions-Comments-Concerns@faa.gov
(405) 954-9510

Approval and Signature

Claire W. Barrett
Departmental Chief Privacy Officer
privacy@dot.gov