



U.S. Department of Transportation
Privacy Impact Assessment
Federal Aviation Administration (FAA)
Designee Management System (DMS)

Responsible Official

Lauren Langston
Email: Lauren.A.Langston@faa.gov
Phone Number: 405-424-8429

Reviewing Official

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





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, regulations, and statutes on behalf of the FAA Administrator.

The FAA developed the Designee Management System (DMS) to have one comprehensive system to manage all designees across Aviation Safety. The DMS standardizes the management lifecycle process of designees and provides the official repository of applicants, along with oversight of appointed designees. DMS collects and maintains Personally Identifiable Information (PII) from applicants seeking designation and appointed designees. In addition, designees may enter information on airmen who are seeking to qualify for a certification.

The FAA is re-publishing this Privacy Impact Assessment (PIA) in accordance with Section 208 of the [E-Government Act of 2002](#) to incorporate managing of the designee's required training previously done by the Designee Registration System (DRS)¹. DRS is no longer operating, and its functionality is now integrated into DMS.

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)

¹ DRS was a web-based training management system that allowed applicants to create user profiles, select and pay for courses through Pay.gov, complete courses via the FAA's Blackboard system, and enabled the FAA to track and manage courses.



examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.²

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

²Office 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).



FAA Administrator. In carrying out its certification responsibilities, the FAA appoints designees to assist in carrying out certifications. 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)

Applicants access DMS through login.gov. The login.gov service, provided by the U.S. General Services Administration (GSA), offers the public secure and private online access to participating government programs. Please review the [Login.gov PIA](#) to obtain additional information.

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)³

³ 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/DA.



- 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 contact⁴
- Designation Type and Location
- Medical License Number/National Provider Identifier⁵
- Upload of supporting documents that may include:⁶
 - Professional resume detailing 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 in 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 applicants who do not meet the qualification requirements, the email advises them to review FAA Order 8000-95D, [Designee Management Policy](#), for qualification requirements. If an applicant feels they meet the qualifications, they can check their answers and resubmit their application.

Applicants seeking to become a designee are required to participate in and successfully complete the initial training program for the designation sought. Completion of initial training is required for applicants seeking a designee appointment, and recurrent training is required to maintain their status. Completion of specialized training permits applicants to achieve higher levels of expertise. For example, designees who conduct medical examinations of people must complete the 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 specialized training must be completed prior to appointment or adding the special authority, and in some cases must be repeated at the interval specified.⁷

⁴ 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.

⁵ The Medical License Number/National Provider Identifier is only required if the applicant is applying for AME.

⁶ Documents uploaded are dependent on the type of certification the applicant is applying for.

⁷ See, [Order 8000.95D, Designee Management Policy](#), Chapter 7, Section 3 (January 21, 2025)



To enroll and pay for a course, an applicant 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. Although the applicant only sees the course amount, the system transmits the other necessary information to Pay.gov to support the transaction. This information is sent encrypted and includes the following: the DMS 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. DMS provides this information to Pay.gov to identify which applicant 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 is transmitted to Pay.gov, applicants 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 an applicant successfully completes their Pay.gov transaction, Pay.gov electronically transmits back to DMS the DMS tracking ID to relate that transaction to a specific applicant, 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.gov⁸ and DMS.

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

Once the Blackboard account is either accessed or created, the applicant may then enroll in their courses within Blackboard. To accomplish this, DMS 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

⁸ See the Pay.gov PIA located <https://fiscal.treasury.gov/files/pia/paygov-pia.pdf> for more information on how the Department of Treasury treats individual information collected or maintained through these payment procedures.



course ID (the catalogue number for the course). After the applicant is successfully enrolled in a course, Blackboard electronically transmits back to DMS an enrollment ID, a system-generated confirmation number for enrollment. This serves as confirmation that the applicant is enrolled in an online course via Blackboard and now has access to complete that specific course.

Finally, when an applicant completes a Blackboard course, they are automatically redirected to their DMS enrollments webpage to view their Blackboard grade and course completion. DMS electronically transmits all applicants' grades from Blackboard per course ID in encrypted form and displays them on the applicant's enrollment webpage. Applicants may view their grades and course completions at their DMS enrollments webpage.

For applicants who 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 includes 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 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 IACRA⁹. 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 and 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.

⁹ This access does not give the designee access to all the airman's records in the FAA.



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) v3¹⁰, 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 Organizations¹¹.

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.

The FAA deploys multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains PII within DMS. DMS collects the applicant's name, suffix, email address, date of birth, airman certification number, gender, country of citizenship, phone number, photo (optional), designee's mailing address (same as personal or business address), and FTN of applicants seeking to become designees in support of designation, certification, and oversight activities. DMS presents applicants with a Privacy Act Statement at the point of collection 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 and Budget (OMB) collection number, OMB 2120-0033.

The FAA retrieves the applicant's information by name and other identifiers. These records are covered by SORN [DOT/FAA 830, Representatives of the Administrator, September 6, 2022, 87 FR 54592](#).

For airmen information received through IACRA or entered by designees in connection with testing activities, FAA relies on applicable upstream notices and public notices governing

¹⁰ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

¹¹ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



those records and uses. This PIA describes how that information is received and used within DMS to document designee activity.

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.

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.

Individuals with active access may update their information directly in DMS. For records originating from or shared with another FAA system, such as IACRA, correction requests may also need to be directed to the source system, as applicable. 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

Additional information about the Department's privacy program may be found at <https://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 it collects, uses, maintains, or disseminates PII.

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 applicant's name, suffix, email address, date of birth, airman certification number, sex, country of citizenship, phone number, photo (optional), designee's mailing address (same as personal or business address), and FTN as part of the application process to become a designee.

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

DMS shares 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.

Federal Aviation Administration Information Management System (FAAMIS) receives the designee's name, designation identification number, designee type, and status, and the information is used to calculate pay grade. In addition, designee's 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 the designee's name, address, city, state, zip code, phone number, country, designee type, and office name.

Aviation Safety Knowledge Management Environment Airworthiness Certification (ASKME AWC) receives the designee's name, designation identification number, and designation status) to verify users are active in DMS. The purpose of this exchange is to verify that an individual has an active designation in DMS.

ATLAS (AAV) exchanges limited designation information with DMS for the purpose of verifying that FAA DMEs are active and authorized to generate standardized mechanic tests.

Blackboard (Bb) receives encrypted student information, including enrollment role and course owner role along with the Blackboard course ID. This exchange allows DMS to confirm enrollment and provide the applicant with access to the specific online course.

Pay.Gov receives the DMS tracking ID, agency ID, application name, and form ID to identify the applicant and the FAA-related payment being submitted. This information enables Pay.Gov to process the applicant's billing details and complete the course payment. After the transaction is successful, Pay.gov sends DMS a tracking ID that links the payment to the applicant and serves as confirmation of the completed payment.

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. FAA reviewed each DMS data element to ensure it is relevant and necessary to determine eligibility, support appointment and oversight, administer training, and document designee activities. Optional fields, such as photo, are identified as optional. Sensitive qualification and background-related fields are collected only where needed to assess eligibility, identity, or specialized authority. To encourage data minimization, the 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.



Applicants' information is retained and disposed of in accordance with NARA-approved retention schedule, [DAA 0237-2020-0013, Designee Case Files](#). Case files consisting of designation application, application letters for appointment as aviation examiner annual renewal agreements, training data, error reports, report cards, and related correspondence are destroyed 25 years after the designee becomes inactive.

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 limits use of PII to applicant evaluation, designee training, appointment and oversight, activity reporting, and authorized disclosures described in the applicable SORN and notices. Access is role-based and limited to users with a need to know. System interfaces and business procedures are configured to share only data needed for the receiving system's authorized function. Access and use are subject to monitoring and review. DMS does not share information with external systems. The sharing of applicants seeking/or assign designees information is conducted in accordance with [DOT/FAA 830 - Representatives of the Administrator, September 6, 2022, 87 FR 54592](#). 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 disclose to members of the public the names, official addresses, and authorizations of those designees who provide FAA certification services, in order to solicit and retain designees for such services.

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](#) and [84 FR 55222, October 15, 2019](#), under "Prefatory Statement of General Routine Uses" (available at <https://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 submission. The DMS also requires applicants to verify/update their application information annually, while appointed designees are subject to the same requirement to retain eligibility for designee status the following year.

Automating the data exchange between DMS and Blackboard ensures data integrity by avoiding human error.

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. FAA employees authenticate with their FAA domain credentials using their personal identity verification 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 login.gov.

Access to DMS is granted on a "need to know" basis. The DMS employs role-based access control, in which user roles have varying levels of access or capabilities. For example, a general user can only perform limited functions, whereas 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.

In the event of a suspected or confirmed privacy incident involving DMS data, FAA follows departmental/FAA incident reporting and response procedures, including prompt reporting, privacy risk assessment, and appropriate notification and mitigation actions.

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.

FAA Order 1370.121B 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 A130, 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 1370.121B, role-based access controls, periodic privacy compliance reviews, and management oversight of records access, retention, and sharing practices. These controls support ongoing assessment of whether DMS handling of PII remains consistent with legal and policy requirements. The FAA will conduct periodic privacy compliance reviews of the DMS as related to the requirements of OMB Circular A-130.

Responsible Official

Lauren Langston
System Owner
Aviation Safety Program Compliance Specialist, AVS

Prepared by: Essie Bell, Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN
Digitally signed by
KARYN MARIE
GORMAN
Date: 2026.09.29
16:24:35 -04'00'