Appendix A: Parts 108/146 Workflows for the Office of Aviation Safety (AVS) Hub

Executive Summary

The Federal Aviation Administration's (FAA) Office of Aviation Safety (AVS) Parts 108 and 146 workflows are a solution within the AVS Hub specifically developed to process permits, certificates, and authorizations under the FAA's Part 108, Beyond Visual Line of Sight (BVLOS) and Part 146, Automated Data Service Providers rule. The Parts 108 and 146 Final Rules were developed in accordance with the Administrator's authority described under 49 U.S.C. Section 106 of subtitle I and pursuant to 49 U.S.C. 44807, *Special Authority for Certain Unmanned Aircraft Systems (UAS),* which permits the FAA Administrator[1] to use a risk-based approach to determine if certain UAS may operate safely in the National Airspace System. Furthermore, the FAA Reauthorization Act of 2024 (section 930 of Pub. L. 118-63) amended 49 U.S.C. chapter 448 by adding § 44811 to require the FAA Administrator to establish performance-based regulations for UAS to be used for beyond visual line of sight (BVLOS) operations. In addition, section 932 of the FAA Reauthorization Act of 2024 directs the FAA Administrator to establish procedures to approve third-party service suppliers. Those include suppliers of UAS Traffic Management (UTM) services to support the safe integration and commercial operation of UAS.

This Privacy Impact Assessment (PIA) was developed pursuant to the E-Government Act of 2002, because the AVS Hub Parts 108 and 146 workflows collect and maintain Personally Identifiable Information (PII) on UAS Operators, Manufacturers, and Automated Data Service Providers (ADSPs) who apply for permits, certificates, and authorizations under the Rule.

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] *See* section 927 of FAA Reauthorization Act of 2024, Pub. L. 118-63.

DOT Privacy Office - Approved 1/09/2026

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 FAA's AVS Parts 108 and 146 workflows are a solution within the AVS Hub specifically developed to process permits, certificates, and authorizations under the FAA's Part 108, Beyond Visual Line of Sight (BVLOS) and Part 146, Automated Data Service Providers. Part 108 establishes a comprehensive framework enabling routine BVLOS UAS operations without the need for case-by-case waivers, setting standards for aircraft design, operators, and operational safety. The operators and manufacturers covered by this part can be individuals or businesses. Part 146 establishes a certification structure for ADSPs that supply the digital traffic management and safety data necessary to support scalable BVLOS activity, including UTM. Like the other groups, ADSPs can be individuals or businesses.

Part 108 introduces two tiers of operating authority: permits for lower-risk, smaller-scale operations and certificates for higher-risk or enterprise operations. Operators must obtain permits or certificates based on operational complexity and report certain data; manufacturers must submit compliance data, including noise and cybersecurity information;

DOT Privacy Office - Approved - 11/04/2026

[2]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).

and ADSPs (under Part 146, below) must secure both organizational certificates and service authorizations.

Depending on the request, the user accesses a different workflow within AVS Hub, as follows:

Parts 108, BVLOS Workflow

BVLOS has general operating requirements, including administrative requirements for operational permitting and certification. Operational requirements depend on the type of request, as follows:

1) Airworthiness Acceptance for Manufacturers

This workflow is used to gather application data for airworthiness acceptance from UAS manufacturers submitting one or multiple declarations of compliance to the FAA. A UAS manufacturer needs to provide information on the operations it has specified, the means of compliance, the standards used, and the various declarations. Information is provided through drop-down boxes and free-text fields. Data elements that are manually input include: manufacturer name, representative name, physical address, telephone number, and email address, UAS make, model, series, serial number, and date of manufacture. Manufacturers also upload documents such as user manuals, design documents, and acceptance standards. These documents are not expected to include additional PII but may include business information such as the manufacturer's representative's name and contact information. Once submitted, an application ID is generated for tracking purposes.

The FAA then reviews the application within the workflow. If they need additional information, they can submit inquiries within the workflow, which generates an email notifying the applicant that an action is required. If the FAA approves a waiver request, a waiver number is issued for the approved waiver application. Airworthiness acceptance is tracked by aircraft serial numbers, while registered manufacturers are tracked by manufacturer names. Information on the waiver is business information only. Once the waiver is issued, A copy of the application and all corresponding data is sent to the Enterprise Data Platform (EDP) for ease of sharing with downstream systems. The applicant is also notified that they have been registered as a manufacturer and that their airworthiness

DOT Privacy Office - Approved - 1/29/2026

acceptance for the UAS they produce, or a waiver for features that exceed the rule, has been issued.

If the application is declined, a notice providing reasoning as well as an email notification is provided to the applicant, who can then log in to the system and view the document citing the reasons for denial.

2) *Permit/Certificate/Authorization for Operators*

An Operator can be an individual or a business. Information that the Operator would need to provide includes reporting procedures, company manual, intended type, training program, communication and ground risk assessments, hazardous materials, and other procedural information. PII includes the applicant's name, address, email address, business contact information (including name and address), as well as UAS serial numbers and UAS registration numbers. Documents that need to be uploaded include flight manuals, safety management and reporting information, recordkeeping plan, communication and ground assessment, and flight information. Business name, representative name, and contact information could be present in these uploaded documents. For a small subset of Operators – those who perform package delivery operations, citizenship information is collected and could include birth certificate, passport, or naturalization document, which could include name, parents' names, place of birth, date of birth, certificate of naturalization number/passport number, marital status, and picture. Once submitted, an application ID is generated for tracking purposes.

The FAA then reviews the application. If they need additional information, they can submit inquiries in AVS Hub, which generates an email notifying the Operator that an action is required. If the FAA approves the request, a permit/certificate/authorization is generated and includes a permit/certificate/authorization number.

Once the certificate is issued, a complete copy of all application documents is sent to the EDP for easier sharing with downstream systems. The Operator is also notified that they can download their certificate/permit/authorization from AVS Hub. If the application is declined, a notice explaining the decision is generated, and an email notification is sent to the Operator, who can log in to the system and view the document.

Records are retrieved by application ID, certificate/permit/authorization number, name, and email address. A small number of Operators are individuals, and their personal information may be reviewed in the context of their application for approval.

Part 146, Automated Data Service Providers Workflow

The Part 146 workflow enables the processing of applications submitted for certifying certain ADSPs. The process allows the ADSP to obtain organizational-level certification and

DOT Privacy Office - Approved 11/04/2016

then obtain authorizations for the individual services they provide. ADSPs are generally businesses, but no regulation or policy prevents an individual from being an ADSP.

When the applicant initiates an application, the Part 146 workflow generates an application ID to track the application. The applicant manually inputs the following information: name and ownership information such as service provider name and associated contact information (principal place of business address, telephone number, email address), ownership information (for corporate entities, the name and address of each stockholder owning 5% or more of the total voting stock of the corporation and if that stockholder is not the sole beneficial owner of the stock, the name of and address of each beneficial owners of the stock, the name and address of each beneficial owner; for non-corporate entities, the name and address of each person having a financial interest in the entity), accountable executive name and associated contact information (address, telephone number, email address).

Additionally, the applicant attests to declarations and uploads documentation demonstrating their authority to conduct business in the United States, which may include PII such as names and contact information (including the names of individuals with titles such as director, principal registered agent, etc.).[3] Certain applicants are required to supplement their declaration attestations with supporting documentation and data, including but not limited to training manuals, reporting procedures, and quality management information.

In addition to the certification information above, the applicant is required to submit an application for at least one part 146 service authorization for the specific automated data service they seek to deploy under their certification. This information includes minimum performance requirements of the service, demonstrations of compliance that the applicant is capable of meeting those minimum performance requirements, demonstrations of compliance with data exchange and software updates requirements, a demonstration that the service supports an aircraft operator's ability to comply with an FAA requirement, and a demonstration that the service is designed in accordance with an industry consensus standard. Once all required information has been provided, the applicant can submit the application to the FAA for processing.

The FAA then reviews the application. If the FAA needs additional information, it can send a request for information, which generates an email to the applicant advising them that an action is required. If the FAA approves the request, a certification number is generated, which includes the certificate service type, any conditions and limitations, the certification

DOT Privacy Office Approved - 11/04/2025

[3] Stockholder and financial request information is used only in specific situations. For example, if at some point in the future a certificate is revoked for non-compliance, the FAA may search to determine if those stockholders or individuals with financial interest in another entity are associated with other certificates. The FAA analyst could search the individual's name and the record retrieved would be other certificates those individuals are associated with. There is not a profile or individual record on these individuals.

date, and a service authorization number (including the service category and service type, any conditions/limitations, and the authorization date) for each authorized service.

If the application is denied, information providing the reason for the denial is generated and an email notification is provided to the applicant with instructions for logging into the system to view the information regarding the denial.

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[4], 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[5].

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 uses multiple methods to ensure applicants are aware of the procedures for submitting various applications and requests, as well as the purposes for which the agency collects and maintains PII. The AVS Hub maintains "Explore Certifications" and "Explore Waivers" web pages that provide information regarding certification and waiver processes. Users can also access a "Resources" web page that provides further information about licensure and certification. Additionally, the FAA previously published the "Normalizing Unmanned Aircraft System (UAS) Beyond Visual Line of Sight (BVLOS) Operations Notice of Proposed Rulemaking (NPRM)" PIA on September 4, 2025.

Records within Parts 108 and 146 workflows are retrieved by a variety of data elements, including application ID, service authorization number, waiver number, certificate/certification number, permit number, name, and email address. The FAA is

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

DOT Privacy Office - Approved - 1/09/2026

published a system of records notice (SORN) titled Department of Transportation, Federal Aviation Administration, DOT/FAA 860 Unmanned Aircraft System Beyond Visual Line of Sight Operations – Parts 108/146 (91 FR 69305 - November 3, 2026).

As required by law, a Privacy Act statement discussing the Department's privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of PII will be available at the initial point of PII collection in the workflows. Lastly, the FAA's publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into Parts 108 and 146 workflows.

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.

Data in the Parts 108 and 146 workflows of AVS Hub is manually entered by the individual whose PII is being requested by the FAA, or by the individual who uploads documents directly. As such, this PII and the documents are relied upon to be accurate and up to date. Privacy Act Statements are present at the point of initial collection of PII and apprise the individual submitting the information of their rights under the Privacy Act.

As such, under the Privacy Act, individuals may request searches to determine whether any records are maintained in the system that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

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 and/or email address
- A description of the records sought, and if possible, the location of the records
- A statement under penalty of perjury that the requester is the individual who he or she claims to be.

DOT Privacy Office - Approved - 11/04/2026

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.

The FAA is required by statute to collect and maintain PII on UAS Operators, business entities, manufacturers, and ADSPs. To issue permits/certificates of authorization to conduct certain BVLOS operations in the NAS, the FAA collects contact information from operators (names, physical addresses, email addresses, and telephone numbers), as well as UAS serial numbers and UAS registration numbers. For a small subset of Operators – those who perform package delivery operations - citizenship information is collected and could include birth certificate, passport, or naturalization document, which could include name, parents' names, place of birth, date of birth, certificate of naturalization number/passport number, marital status, and photograph. Once submitted, an application ID is generated for tracking purposes. If the FAA approves the request, a permit/certificate is generated and includes a permit/certificate number.

The application data for airworthiness acceptance from UAS manufacturers submitting declarations of compliance to the FAA includes manufacturers' contact information (names, physical addresses, email addresses, and telephone numbers) and aircraft information (serial number and registration number), among other details. Once an application is submitted, an application ID is generated for tracking purposes. If the FAA approves the request, a waiver number is issued for approved waiver applications. Airworthiness acceptance is tracked by aircraft serial numbers, while registered manufacturers are tracked by manufacturer name.

Finally, to certify ADSPs as well as their automated data services, part 146 requires the collection of ADSP contact information, including names, physical addresses, email addresses and telephone numbers. When the applicant initiates an application, an application ID is generated to track it. If the FAA approves the application, a certification number and if applicable, a service authorization number is generated.

The requirement to collect the PII is issued under the authority of Section 106 of subtitle I of title 49, the Federal Aviation Administration, which describes the authority of the FAA Administrator. The associated UAS BVLOS rulemaking is issued under the authority described in 49 U.S.C. 44807, *Special authority for certain UAS*, which permits the FAA Administrator[6] to use a risk-based approach to determine if certain UAS may operate safely in the NAS. Furthermore, the FAA Reauthorization Act of 2024 (section 930 of Pub. L. 118-63), amended 49 U.S.C. chapter 448 by adding § 44811, requires the FAA Administrator to establish performance-based regulations for UAS to be used for BVLOS operations. The

[6] *See* section 927 of FAA Reauthorization Act of 2024, Pub. L. 118-63.

DOT Privacy Office - Approved - 11/04/2025

FAA Administrator must, at a minimum, establish acceptable risk levels for BVLOS operations; standards for remote pilots or UAS operators; an approval or acceptance process for UAS which may leverage special airworthiness certificates (SAC) or a manufacturer declaration of compliance (DOC) process; operating rules for UAS that are approved or accepted; protocols of networked information; and safety of manned aircraft operating in the NAS. Furthermore, section 932 of the FAA Reauthorization Act of 2024 directs the FAA Administrator to establish procedures, including rulemaking, to approve third-party service suppliers. Those include suppliers of UTM services to support the safe integration and commercial operation of UAS. The rulemaking and subsequent regulations that are covered by this system of records are within the scope of these authorities.

AVS Hub Parts 108 and 146 share a complete copy of the application, certificate, and waiver data (including the PII referenced in the System Overview) with the Enterprise Data Platform (EDP). This sharing is for the ease of sharing information within the FAA.

Data Minimization & Retention

The FAA manages privacy risk by minimizing the amount of PII collected to support the permits, certificates, and authorizations processed under the FAA's Part 108, Beyond Visual Line of Sight (BVLOS) and Part 146, Automated Data Service Providers through the creation of a standardized process. Individuals utilizing Parts 108 and 146 workflows complete a fillable electronic web form that specifies which data should be input. Radio buttons, checkboxes and dropdown boxes all help prevent individuals from adding unnecessary PII to the workflow. Individuals are also specifically advised which documents to upload. AVS Hub also provides links to various educational materials on licensure and certification that offer guidance on required documentation.

All records relating to the AVS Hub Parts 108 and 146 workflows are currently maintained as permanent until a new schedule is approved by the National Archives and Records Administration.

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.

The FAA published a SORN titled Department of Transportation, DOT/FAA 860 Unmanned Aircraft System Beyond Visual Line of Sight Operations – Parts 108/14691 (FR 69305 - November 3, 2026). 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) as follows:

DOT Privacy Office - Approved - 11/04/2026

1. To the public, in the case of part 108, waiver applications and decisions, including any history of previous, pending, existing, or denied requests for waivers applicable to the UAS at issue for purposes of the waiver, and special provisions applicable to the UAS operation that is the subject of the request. Individual or business names will be shared as needed. Email addresses and telephone numbers will not be disclosed pursuant to this Routine Use. Airspace authorizations that the FAA issues will also not be disclosed pursuant to this Routine Use, except to the extent that an airspace authorization is listed or summarized in the terms of a waiver.

2. To the public, in the case of part 146, the FAA manages a public-facing web page that provides the following information associated with each part 146 certification: (1) the service provider name, (2) the service type of the certification, and (3) the service type and category for each authorized part 146 service associated with the certification.

3. To law enforcement, when necessary and relevant to an FAA enforcement activity.

4. To the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.

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

critical infrastructure protection.

6. To the Transportation Security Administration (TSA), when necessary and relevant to the execution of TSA's duty to impose security measures on related operations, assess security risks, enforce compliance, conduct security threat assessments, and for the purpose of vetting individuals and operators.

DOT may also disclose Parts 108/146 information outside DOT pursuant to 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published on DOT's General Routine Uses SORNs page.

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).

Parts 108 and 146 workflows within AVS Hub collect information directly from the individual UAS Operator, Manufacturer, or ADSP representative. As the information is manually entered into the web forms by the applicant, it is assumed to be correct, and errors are expected to be minimal. Technical features built into the forms, such as formatted text

DOT Privacy Office - Approved 11/04/2026

boxes and drop-down menus, support data quality. During the electronic file transfer from AVS Hub to EDP, there is no human interface, which eliminates the possibility of human error possibly impacting the quality of the data.

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.

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 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020.

AVS Hub Parts 108 and 146 workflows employ specific administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Personnel can only access the internal interfaces via the FAA's network using their Personal Identity Verification (PIV) card. All PII is encrypted in transit and at rest. Personnel receive guidance on their duties related to collecting, using, processing, and securing PII. This includes mandatory annual security and privacy awareness training, as well as a review of the FAA Rules of Behavior. The DOT and FAA Privacy Office conduct periodic privacy compliance reviews of AVS Hub in accordance with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

AVS Hub has a system security plan in place. The system was issued an Authority to Operate in May 2026 after completing the authorization and accreditation process that reviews security controls and procedures, and that validates that AVS Hub is compliant with appropriate information security processes and policies

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.

DOT Privacy Office - Approved - 1/6/2026

FAA Order 1370.121B, FAA Information Security and Privacy Program & Policy, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. In addition to these practices, the FAA implements additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with AVS Hub are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B. As previously stated, the FAA conducts periodic privacy compliance reviews of the AVS Hub as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Sherry Christeson
System Owner

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.11.04 15:49:42 -05'00'

DOT Privacy Office - Approved - 11/04/2026