This document is scheduled to be published in the
Federal Register on 2026-11-03 and available online at
https://www.federalregister.gov/d/2026-22436, and on
https://govinfo.gov

DEPARTM

Office of the Secretary

[Docket No. DOT-OST-2026-3862]

Privacy Act of 1974; System of Records

AGENCY: Federal Aviation Administration (FAA), U.S. Department of Transportation.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the United States Department of Transportation (DOT) proposes a new system of records titled, "Department of Transportation, Federal Aviation Administration DOT/FAA 860, Unmanned Aircraft System Beyond Visual Line of Sight Operations – Parts 108/146." This system of records allows the FAA to collect, use, and maintain information from operators, manufacturers and Automated Data Service Providers (ADSPs), to the extent the operator, manufacturer or ADSP is an individual, when requesting authorizations to conduct or support certain beyond visual line of sight operations in the United States national airspace (NAS).

DATES: Submit comments on or before [*INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION DATE IN THE FEDERAL REGISTER]*. The Department may publish an amended Systems of Records Notice (hereafter "Notice") in light of any comments received. This new system will be effective immediately. The routine uses will be effective [*INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER*].

ADDRESSES: You may submit comments identified by docket number DOT-OST-2026-3862 by any of the following methods:

- *Federal e-Rulemaking Portal:* https://www.regulations.gov. Follow the instructions for submitting comments.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE. West Building Ground Floor, Room W58–213, Washington, DC 20590–0001.

- *Hand Delivery or Courier:* West Building Ground Floor, Room W12–140, 1200 New Jersey Ave. SE, between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- *Fax:* (202) 493–2251.

Instructions: You must include the agency name and docket number DOT-OST-2026-3862. All comments received will be posted without change to https://www.regulations.gov, including any personal information provided.

Privacy Act: Anyone is able to search the electronic form of all comments received in any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.).

Docket: For access to the docket to read background documents or comments received, go to https://www.regulations.gov or to the street address listed above. Follow the online instructions for accessing the docket.

FOR FURTHER INFORMATION CONTACT: For questions, please contact: Karyn Gorman, Departmental Chief Privacy Officer, Privacy Office, Department of Transportation, Washington, DC 20590; privacy@dot.gov; or 202-603-8321.

SUPPLEMENTARY INFORMATION:

Background

The Normalizing Unmanned Aircraft Systems (UAS) Beyond Visual Line of Sight (BVLOS) Operations final rule was issued under the authority of 49 United States Code (U.S.C.). Section 106. The associated rulemaking was issued under the authority described in 49 U.S.C. 44807, *Special authority for certain UAS*, which permitted the FAA Administrator[1] 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.

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

chapter 448 by adding § 44811 to require the FAA to establish performance-based regulations for UAS to be used for BVLOS operations. The UAS operations BVLOS regulations established acceptable risk levels for BVLOS operations; standards for remote pilots or UAS operators; an approval or acceptance process for UAS which leveraged special airworthiness certificates (SAC) or a manufacturer declaration of compliance (DOC); operating rules for UAS that were 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 required procedures, including rulemaking, to approve third-party service suppliers. This included suppliers of UAS Traffic Management (UTM) services to support the safe integration and commercial operations of UAS. The rulemaking and subsequent regulations that are covered by this system of records are within the scope of these authorities.

This rulemaking established parts 108 *Operations of Unmanned Aircraft Systems Beyond Visual Line of Sight,* and 146 *Automated Data Service Providers*. Part 108 established a comprehensive framework enabling routine UAS Operations BVLOS 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 established a certification structure for Automated Data Service Providers (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 introduced two tiers of operating authority: permits for lower-risk, smaller-scale UAS operations and certificates for higher-risk or enterprise UAS operations. To administer this system, the FAA developed an information portal for manufacturers, operators, and ADSPs. Operators must obtain permits or certificates based on operational complexity and report certain data; manufacturers may be required to submit compliance data, including noise and cybersecurity information; and ADSPs must secure both organizational certificates and service-

specific authorizations. As a result, the FAA collects identifying and technical data from all the aforementioned participants within the BVLOS ecosystem.

To issue permits/certificates of authorization to conduct certain BVLOS operations in the NAS, the FAA collects contact information (names, physical addresses, email addresses, and telephone numbers) from operators, 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 identification number (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 number, while registered manufacturers are tracked by manufacturer's name.

Finally, part 146 introduces the mechanisms and requirements to certify ADSPs and their automated data services. This process requires ADSPs to obtain organizational-level certificates and subsequently obtain authorizations for the individual services they provide. These applicants would also provide their contact information (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 is generated.

Privacy Act

The Privacy Act (5 U.S.C. 552a) governs how the Federal Government collects, maintains, and uses personally identifiable information (PII) in a System of Records. A "System of Records" is a group of any records under the control of a federal agency from which information about individuals is retrieved by name or other personal identifier. The Privacy Act requires each agency to publish in the ***Federal Register*** a System of Records Notice (SORN) identifying and describing each System of Records the agency maintains, including the purposes for which the agency uses PII in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals to whom a Privacy Act record pertains can exercise their rights under the Privacy Act (*e.g.,* to determine if the system contains information about them and to contest inaccurate information). In accordance with 5 U.S.C. 552a(r), DOT has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

DOT/FAA 860 Unmanned Aircraft System Beyond Visual Line of Sight Operations – Parts 108/146.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Located in the FAA Cloud Services Amazon Web Services (FCS AWS) East West Public Cloud.

SYSTEM MANAGER(S):

AVS Hub Owner, AFB-260, Federal Aviation Administration, 6961 Flight Road, Riverside, CA 92504; Email: 9-AVS-AFB260-STIM@faa.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. Sect. 106 subtitle I; 49 U.S.C. 44807; 49 U.S.C. 44811; and the FAA Reauthorization Act of 2024 (sections 930 and 932).

PURPOSE(S) OF THE SYSTEM:

To allow the FAA to collect, use, and maintain information from individuals acting as or representing operators, manufacturers, and ADSPs when they request authorizations to conduct or support certain BVLOS operations in the NAS and/or airworthiness acceptance to manufacture compliant UAS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

For part 108, records cover individuals acting as or representing UAS operators requesting a permit or certificate to conduct operations, and individuals acting as or representing manufacturers seeking airworthiness acceptance for UAS. For part 146, records cover individuals acting as or representing the ADSPs, corporate stockholders who own 5% or more of the corporation's total voting stock, non-corporate persons with a financial interest in the entity, and accountable executives.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system apply to individuals acting as or representing operators, manufacturers, and ADSPs as follows:

Operators

These records include name, physical address, email address, and telephone number, the address of the principal base of operations, if different from the address provided for contact information, name of the individual who serves as operations supervisor, application ID, permit/ certificate number, UAS serial number and UAS registration number. For a small subset of operators 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.

Manufacturers

These records include the manufacturer's name, physical address, telephone number, email address, application ID, and waiver number; the unmanned aircraft make, model, series, serial number, and date of manufacture.

Automated Data Service Providers

These records include name, physical address, mailing address, telephone number, email address, application ID, certification number and service authorization number; for corporate applicants: name and physical address of each stockholder who owns 5% or more of the total voting stock of the corporation; for non-corporate applicants: name and physical address of each person having a financial interest in the entity; name, mailing address, telephone number and email address of each accountable executive.

RECORD SOURCE CATEGORIES:

Records are obtained from individuals authorized to operate UAS, manufacture UAS, or offer automated data services to UAS operators, as well as FAA personnel logging actions associated with various activities, including, but not limited to, certification, authorization, oversight, and enforcement.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

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:

System-Specific Routine Uses:

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 webpage 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.

Departmental Routine Uses:

7. In the event that a system of records maintained by DOT to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.

8. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DOT decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

9. A record from this system of records may be disclosed, as a routine use, to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

10a. Routine Use for Disclosure for Use in Litigation. It shall be a routine use of the records in this system of records to disclose them to the Department of Justice or other Federal agency conducting litigation when (a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof (including a member of the Coast Guard), in his/her official capacity, or (c) Any employee of DOT or any agency thereof (including a member of the Coast Guard), in his/her individual capacity where the Department of Justice has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that litigation is likely to affect the United States, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or other Federal agency conducting the litigation is deemed

by DOT to be relevant and necessary in the litigation, provided, however, that in each case, DOT determines that disclosure of the records in the litigation is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

10b. Routine Use for Agency Disclosure in Other Proceedings. It shall be a routine use of records in this system to disclose them in proceedings before any court or adjudicative or administrative body before which DOT or any agency thereof, appears, when (a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof in his/her official capacity, or (c) Any employee of DOT or any agency thereof in his/her individual capacity where DOT has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that the proceeding is likely to affect the United States, is a party to the proceeding or has an interest in such proceeding, and DOT determines that use of such records is relevant and necessary in the proceeding, provided, however, that in each case, DOT determines that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

12. Disclosure may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. In such cases, however, the Congressional office does not have greater rights to records than the individual. Thus, the disclosure may be withheld from delivery to the individual where the file contains investigative or actual information or other materials which are being used, or are expected to be used, to support prosecution or fines against the individual for alleged violations of a statute, or of regulations of the Department based on statutory authority. No such limitations apply to records requested for Congressional oversight or legislative purposes; release is authorized under 49 CFR 10.35(9).

13. One or more records from a system of records may be disclosed routinely to the National Archives and Records Administration in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

14. It shall be a routine use of the information in any DOT system of records to provide to the Attorney General of the United States, or his/her designee, information indicating that a person meets any of the disqualifications for receipt, possession, shipment, or transport of a firearm under the Brady Handgun Violence Prevention Act. In case of a dispute concerning the validity of the information provided by DOT to the Attorney General, or his/her designee, it shall be a routine use of the information in any DOT system of records to make any disclosures of such information to the National Background Information Check System, established by the Brady Handgun Violence Prevention Act, as may be necessary to resolve such dispute.

15a. To appropriate agencies, entities, and persons when (1) DOT suspects or has confirmed that there has been a breach of the system of records; (2) DOT has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOT (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOT's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

15b. To another Federal agency or Federal entity, when DOT determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

16. DOT may disclose records from this system, as a routine use, to the Office of Government Information Services for the purpose of (a) resolving disputes between FOIA requesters and Federal agencies and (b) reviewing agencies' policies, procedures, and compliance in order to recommend policy changes to Congress and the President.

17. DOT may disclose records from this system, as a routine use, to contractors and their agents, experts, consultants, and others performing or working on a contract, service, cooperative agreement, or other assignment for DOT, when necessary to accomplish an agency function related to this system of records.

18. DOT may disclose from this system, as a routine use, records consisting of, or relating to, terrorism information (6 U.S.C. 485(a)(5)), homeland security information (6 U.S.C. 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment, November 22, 2006) to a Federal, State, local, tribal, territorial, foreign government and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to detect, prevent, disrupt, preempt, and mitigate the effects of terrorist activities against the territory, people, and interests of the United States of America, as contemplated by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458) and Executive Order 13388 (October 25, 2005).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored in electronic form. Electronic records are stored in a database with appropriate security and access limitation.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records can be accessed by both internal and external users to the FAA upon authentication into the system. Based on their business need, users can retrieve records by application ID, service authorization number, waiver number, certificate/certification number, permit number, name, and email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

FAA is actively working on drafting the appropriate records retention schedule(s) to be submitted to NARA by the latter part of fiscal year 2027. Until these schedules are approved by NARA, all records in this system will be treated as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT and FAA automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

Individuals seeking notification of whether this system of records contains information about them may contact the System Manager at the address provided in the section ‘‘System Manager’’. When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform to the Privacy Act regulations set forth in 49 CFR part 10. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest the content of any record pertaining to them in the system of records may contact the System Manager and follow the Privacy Act procedures in 49 CFR part 10, subpart E, Correction of Records. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made

under penalty of perjury as a substitute for notarization. If your request contests the content of records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

NOTIFICATION PROCEDURES:

See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

No exemptions claimed.

HISTORY:

None.

Issued in Washington, DC.

Karyn Gorman,
Departmental Chief Privacy Officer.

Billing Code No. 4910-9X

[FR Doc. 2026-22436 Filed: 11/2/2026 8:45 am; Publication Date: 11/3/2026]