U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

FAA

Normalizing Unmanned Aircraft System (UAS) Beyond Visual Line of Sight (BVLOS) Operations Notice of Proposed Rulemaking (NPRM)

Responsible Official

Michelle Ferritto
Email: 9-FAA-UAS-BVLOS-Rule@faa.gov
Phone Number: (844) 359-6982

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) developed this Privacy Impact Assessment (PIA) for the Normalizing Unmanned Aircraft System (UAS) Beyond Visual Line of Sight (BVLOS) Operations notice of proposed rulemaking (NPRM) (Rulemaking Identification Number 2120-AL82) (herein, the "BVLOS NPRM" or "this NPRM"). This proposed rule would establish requirements for conducting unmanned aircraft systems (UAS) beyond visual line of sight (BVLOS) operations in United States airspace. This action would normalize certain low altitude UAS operations and expedite the introduction of BVLOS UAS operations in the national airspace system (NAS), while ensuring the safety and efficiency of United States airspace.

Many, though not all, operations under the proposed part 108 are anticipated to be commercial. The FAA developed this PIA in accordance with the E-Government Act of 2002 because the NPRM proposes the collection of information from respondents who may be individuals or businesses.

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

[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).

electronic information systems and collections handle 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

This proposed rulemaking is to be issued under the authority described in title 49 of the United Sates Code (49 U.S.C.) subtitle VII, part A, subpart iii, section 44807, *Special authority for certain unmanned aircraft systems*, which permits the Administrator of the FAA to use a risk-based approach to determine if certain UAS may operate safely in the NAS. Section 44807(b) provides a list of factors that the Administrator must consider when determining which types of UAS may operate safely in the NAS, including size, weight, speed, operational capability, proximity to airports and populated areas, operation over people, operation within visual line of sight, or operation during the day or night. Section 44807(b) further requires the Administrator to consider whether a certificate under 44703 or 44704 of this chapter, or a certificate of waiver or authorization is required. Per section 44807(c), when the Administrator determines that certain UAS may operate safely in the NAS, the Administrator must then "establish requirements for the safe operation of such aircraft systems in the national airspace system." This regulation is within the scope of that authority.

Furthermore, this proposed rulemaking is promulgated pursuant to 49 U.S.C. 40103(b)(1) and (2), which directs the FAA to issue regulations: (1) to ensure the safety of aircraft and the efficient use of airspace; and (2) to govern the flight of aircraft for purposes of navigating, protecting and identifying aircraft, and protecting individuals and property on the ground. In addition, 49 U.S.C. 44701(a)(5) charges the FAA with promoting safe flight of civil aircraft by prescribing regulations the FAA finds necessary for safety in air commerce and national security.

In 2024, Congress passed the FAA Reauthorization Act of 2024 (Pub. L. No. 118-63). Section 930 of Pub. L. 118-63 directs the FAA Administrator to issue a NPRM and

subsequent final rule establishing a performance-based regulatory pathway for UAS to operate BVLOS. Additionally, section 932 directs the FAA Administrator to establish procedures to approve third-party service suppliers of UAS traffic management. As part of its ongoing efforts to integrate UAS operations into the NAS, and pursuant to 49 U.S.C. 44807, the FAA Administrator is proposing to amend FAA regulations to adopt specific rules for BVLOS operations of UAS in the NAS.

Furthermore, on June 6, 2025, the President signed Executive Order No. 14307, *Unleashing American Drone Dominance,* which directs that "the Secretary of Transportation, acting through the Administrator of the FAA, shall issue a proposed rule enabling routine BVLOS operations for UAS for commercial and public safety purposes.[2]"

Proposal

The BVLOS NPRM would include new operational requirements for unmanned aircraft (UA) with airworthiness acceptance, enabling routine BVLOS operations without waivers or exemptions. These general operating requirements include the administrative requirements for the two tiers of operational authorization, permits and certificates. Permitted operations would allow operators to conduct certain BVLOS operations using a streamlined approach under a permit issued by the FAA. Those conducting higher risk threshold operations, due to size, weight, speed, or other parameters, would instead need to seek operational certification. Proposed part 108 would detail the requirements for airworthiness acceptance, operating rules, operating personnel, and the operating permits and certificates.

Under this NPRM, strategic deconfliction and conformance monitoring would be key to the successful integration of UAS into the NAS and would be a requirement for several categories of operations. As such, this action would create a defined regulatory approval pathway for third-party services, provided by entities that would be known as 'automated data service providers,' which would include UAS Traffic Management (UTM) service suppliers. Proposed part 146 would certify and authorize automated data service providers that would manage UAS traffic and information necessary for safe and efficient operation of the NAS.

Information System

To implement the proposed rulemaking, if issued as a Final Rule, the FAA would develop an information system that would include portals for three distinct groups of users. This information system would include an airworthiness acceptance portal for manufacturers, a permit/certificate/authorization portal for operators, and a certificate/authorization portal for

[2] 90 FR 24727.

automated data service providers. These portals, and the information system writ large, would facilitate the FAA's ingestion of information required for submission as described in proposed parts 108 and 146. Users of this information system would need to establish an online account with the FAA to access any of or all three portals.

Use of Information System by UAS Manufacturers

This system would be used to gather application data for airworthiness acceptance from UAS manufacturers submitting one or multiple declaration(s) of compliance to the FAA. The manufacturers' portal would have to provide a context sensitive, menu-based process for applicants to answer questions related drone design, operational type, means of compliance, and other information FAA would need to evaluate to assess declarations of compliance. Under proposed § 108.715(b), a declaration of compliance must include the following, be signed by the manufacturer's authorized representative or agent, and be submitted to the FAA via the portal:

> (1) The manufacturer's name, physical address, telephone number, and email address.
>
> (2) The unmanned aircraft make, model, series, serial number, and date of manufacture.
>
> (3) The operations the manufacturer has specified may be safely conducted using the unmanned aircraft system.
>
> (4) The means of compliance used to determine the unmanned aircraft system's compliance with design, test, production, and airworthiness requirements of subparts G and H of this part.
>
> (5) The means of compliance for noise or other method of compliance specified in part 36 used for compliance used to determine the unmanned aircraft system's compliance with noise requirements.
>
> (6) The standard used, if another standard acceptable to the Administrator is used to meet the cybersecurity requirements of proposed § 108.875.
>
> (7) A declaration that the unmanned aircraft system meets the requirements of proposed § 108.705.
>
> (8) A declaration that the determination required by paragraph (b)(7) of this section was made by an individual who meets the requirements of proposed § 108.710(c).
>
> (9) A declaration that the unmanned aircraft system conforms to the manufacturer's design data and that the manufacturer used a quality assurance system that meets the requirements of § 108.730.

(10) A declaration that the manufacturer will make available to any registered owner, the National Transportations Safety Board (NTSB), or the Administrator the documents specified in proposed § 108.720 upon request.

(11) A declaration that the manufacturer will support the unmanned aircraft systems after airworthiness acceptance by implementing and maintaining a documented continued operational safety program as required in proposed § 108.740.

(12) A declaration that the manufacturer will monitor and correct safety-of-flight issues through the issuance of safety bulletins following airworthiness acceptance.

(13) A declaration that the manufacturer has inspected the unmanned aircraft system in accordance with proposed § 108.735.

(14) A declaration that at the request of the Administrator, the manufacturer will provide unrestricted access to its facilities and to all data and documentation and allow the Administrator to witness any tests necessary to determine compliance with this section or other applicable requirements of this chapter, or other information as requested by the Administrator.

(15) A declaration that the manufacturer has established and will maintain a quality assurance system that meets the requirements of proposed § 108.730.

(16) A declaration that the UAS complies with subpart F of part 89.

Use of Information System by UAS Operators

Under proposed part 108, operators of UAS seeking to operate under the proposed rule would need to first obtain an operating permit or certificate from the FAA. An operating permit or certificate would enable that operator to perform a specific type of operation with the UAS. Generally, under the proposed rule, an operating permit would be the appropriate permission for smaller, less-complex operations, and an operating certificate would be the appropriate permission for larger, more-complex operations.

The applications for permit or certificate would be solely online using a portal designed for operator users within the information system described herein. The operator would be either an individual or a business. The information that would be required to be submitted in an application for an operating certificate is found in proposed §108.505; likewise, the information that would need to be submitted for an operating permit is found in proposed § 108.405. The list of required information is found below. In addition to a description of the operation, items (1) through (9) and (17) would be required for both operating permits and certificates under the proposed rule; items (10) through (16) would be only required for operating certificates under the proposed rule:

(1) The applicant's name and contact information (physical address, email address, and telephone number).

(2) Address of the principal base of operations, if different from the address provided for contact information, in accordance with proposed § 108.30.

(3) Name of the individual who serves as operations supervisor, in accordance with proposed § 108.305.

(4) The intended type of UAS operations, in accordance with proposed § 108.400(a) or 500(a).

(5) The intended area(s) of operation, in accordance with proposed § 108.165.

(6) Company manual(s), as required under proposed § 108.135.

(7) A recordkeeping plan as required under proposed § 108.40.

(8) Operator reporting procedures, as required under proposed § 108.45.

(9) The type(s) of unmanned aircraft to be used in operations that comply with the requirements of proposed § 108.105.

(10) A training program, as required under proposed §§ 108.540 and 108.315.

(11) Communication and ground risk assessments, as required under proposed § 108.550.

(12) Safety management system, as required under proposed § 108.560.

(13) Hazardous materials procedures, information, and training program, as required under proposed § 108.570.

(14) Procedures permitting the use of inoperative equipment, pursuant to proposed § 108.555.

(15) Plan for complying with duty and rest requirements, pursuant to proposed § 108.330.

(16) For those operators proposing to engage in package delivery, documentation of their citizenship status under proposed § 108.505.

(17) Additional information the Administrator may determine is necessary to evaluate the application.

Operators would also be required to report flight data (including the total flight hours and the make/model/series for each UA), UAS serial numbers and registration, interruption reports, service difficulty reports, security occurrences, emergency conditions, and other event information under the proposed rule. It is anticipated that such reporting would occur through this same portal/information system described herein. Reporting requirements are proposed in § 108.45.

Operators who seek authorization to deviate from certain regulations under proposed part 108 would need to additionally apply for authorization under the proposed rule. Such

applications would also be submitted using the same portal system as the application for an operator permit/certificate.

Further, operations supervisors, flight coordinators, and other covered personnel would be required to obtain up to a Level 3 security threat assessment conducted by TSA under proposed § 108.335. [3] All data under this part is solely the responsibility of the Transportation Security Administration (TSA), as it is neither collected nor retained by the FAA. Likewise, operators proposing to engage in package delivery would be required to contact the Transportation Security Administration (TSA) and request and obtain a limited security program equivalent with 49 CFR 1544.101(g), under proposed §§ 108.440(i) and 108.565(f). All data under this proposed section would solely be the responsibility of TSA and would neither be collected nor retained by the FAA.

Use of Information System by Automated Data Service Providers

In addition, this FAA platform would also enable the processing of applications submitted for certificating certain automated data service providers as well as their automated data services that are subject to requirements proposed in part 146. To maximize flexibility without sacrificing safety, the FAA anticipates constructing a two-part application process under part 146. This process would require the automated data service provider to obtain a certificate at the organizational level, and then obtain authorizations for the individual services they provide.

To be certificated at the organizational level, applicants would be required to submit the following certification information into the FAA platform:

1. Applicant information, which would include their name, contact information, as well as ownership information.

2. Service Level certification information, which entails data and documentation the applicant must submit-- depending on the service level-- demonstrating the applicant's ability to comply with the minimum requirements of the rule. These data

[3] In regards to any vetting conducted by TSA, the security threat assessments proposed in this NPRM are covered by a current Department of Homeland Security system of records titled, "Department of Homeland Security/Transportation Security Administration--002 Transportation Security Threat Assessment System of Records." This system of records allows TSA to collect and maintain records related to security threat assessments, employment investigations, and evaluations that TSA conducts on certain individuals for security purposes. For example, individuals who apply for a Transportation Worker Identification Credential or a Hazardous Materials Endorsement must undergo a security threat assessment, and records associated with the assessment are covered by this system.

and documentation pertaining to the minimum requirements include the submission of information pertaining to the applicants training, reporting procedures, quality management system, and change management system.

3. For certain foreign qualified applicants only, a part 146 equivalent certification issued to the automated data service provider by the foreign civil aviation authority with whom the FAA has a bilateral agreement. The FAA would assess information provided by such applicants on a case-by-case basis.

In addition to the certification information above, the applicant would also be required to submit an application for an FAA authorization regarding the specific automated data service they seek to deploy under their certificate. To do so, applicants are required to submit the following information to the FAA platform, which also depends on the service level.

1. The minimum performance requirements for the specific automated data service they seek to deploy into the NAS.

2. Proof that the applicant is capable of meeting the minimum performance requirements of the requested automated data service.

3. Proof that the automated data service meets that the data exchange requirements (i.e., the service is interoperable, employs safeguards; is authenticated; and use non-repudiation methods) AND that the service software updates procedures are in compliance with FAA requirements.

4. Proof that the automated data service is designed in accordance with a published industry consensus standard.

5. Proof that the automated data service supports aircraft operations to comply with requirements in chapter I of 14 CFR.

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

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

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 is publishing this PIA to inform the public of the privacy risks and mitigation strategies associated with the FAA's collection, use, dissemination, and retention of PII resulting from the NPRM. To meet the requirements of the proposed rulemaking, if the proposed rulemaking were issued as a Final Rule, a new system would be developed that would gather application data for airworthiness acceptance from UAS manufacturers, including a means of compliance and a declaration of compliance. The FAA would develop a PIA for this new system that would be published to provide notice.

It has not been determined whether records would be retrieved by a unique identifier; however, if they are, and are therefore considered Privacy Act records, the FAA would provide notice through the applicable Privacy Act System of Records.

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.

If it is determined that new systems records are afforded protection under the Privacy Act, under the provisions of the Privacy Act, individuals may request searches of records within the new system to determine if any records within that system pertain to them. Individuals wishing to know if their records appear in this new system may inquire in writing to:

Federal Aviation Administration
Privacy Office

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

800 Independence Ave. SW
Washington, DC 20591

Included in the request must be the following:

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

Contesting record procedures:

Individuals wanting to contest information about themselves contained in this system must make their requests in writing. The written request must provide details supporting the requested correction to the record. The request must be mailed to the following address:

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

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

This NPRM would establish requirements for conducting UAS BVLOS operations in United States airspace, and any PII that would be collected pursuant to a Final Rule would be collected to further this purpose.

This rulemaking is issued under the authority described in subtitle VII, part A, subpart iii, section 44807, Special authority for certain unmanned aircraft systems, which permits the Secretary of Transportation to use a risk-based approach to determine if certain UAS may operate safely in the NAS. In addition, the following authorities provide the legal basis for issuing this notice of proposed rulemaking and the collection of PII that could result after issuance of the Final Rule:

- 49 U.S.C. 40103(b)(1) and (2) directs the FAA to issue regulations: (1) to ensure the safety of aircraft and the efficient use of airspace; and (2) to govern the flight of aircraft for purposes of navigating, protecting and identifying aircraft, and protecting individuals and property on the ground.
- 49 U.S.C. 44701(a)(5) charges the FAA with promoting safe flight of civil aircraft by prescribing regulations the FAA finds necessary for safety in air commerce and national security.

- The FAA Reauthorization Act of 2024 (Pub. L. No. 118-63). Specifically, section 930 of Public Law 118-63 directs the FAA Administrator to issue a NPRM and subsequent final rule establishing a performance-based regulatory pathway for UAS to operate BVLOS. Additionally, section 932 directs the FAA Administrator to establish procedures to approve third-party service suppliers of UAS traffic management.
- Executive Order No. 14307, *Unleashing American Drone Dominance*, which directs that "the Secretary of Transportation, acting through the Administrator of the FAA, shall issue a proposed rule enabling routine BVLOS operations for UAS for commercial and public safety purposes.[6] A final rule shall be published within 240 days of the date of this order, as appropriate." FAA is publishing this proposed rule to fulfill that directive.

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.

This NPRM proposes the collection of information discussed in the Overview that is relevant and necessary to enable BVLOS UAS operations. Pursuant to this NPRM, the information the FAA is proposing to collect is the minimum amount of information necessary for the FAA to fulfill its purpose of enabling certain BVLOS operations. If a Final Rule is published, the FAA would ultimately develop a new IT system to meet the requirements of the NPRM. If and when the FAA begins to collect information through that IT system or through other mechanisms, a PIA would be published that would include a full discussion about Data Retention.

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.

This PIA describes collections for an NPRM, so no PII is being collected at this time. If the proposed rule is ultimately published as a Final Rule, a new IT system would be developed to meet the requirements of the NPRM. The new system would not share any information externally unless disclosure is required by law and would only use PII in a manner that is

[6] 90 FR 24727.

compatible with the reason for which it was collected. If and when the FAA begins to collect information through that IT system or through other mechanisms, a PIA would be published that would include a full discussion about information use limitations.

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).

Because this PIA describes a proposed rulemaking, no PII is being collected at this time. If the FAA collects information from manufacturers in the future, it would take steps to ensure that is accurate, relevant, timely and complete. The FAA would publish a PIA for any new IT system that it develops to collect and maintain information, and that PIA would include a full discussion about Data Quality and Integrity.

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.

No PII is currently being collected associated with this NPRM. However, generally, the FAA protects PII by 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 System Management Act (FISMA). The safeguards 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 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, 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, if the NPRM is finalized as proposed, the FAA would implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with information that might ultimately be collected would receive clear guidance about their duties related to collecting, using, and processing privacy data. Mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B, provide additional guidance. The FAA conducts periodic privacy compliance reviews of all information systems consistent with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Michelle Ferritto
Director, Airmen and Airspace Rules Division, Office of Rulemaking

Prepared by: Barbara Stance, Chief 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: 2025.09.03 08:51:53 -04'00'