



U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA) Low Altitude Authorization and Notification Capability (LAANC)

Responsible Official

Casey Nair

LAANC Program Manager

casey.nair@faa.gov

Reviewing Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

privacy@dot.gov



Executive Summary

Individual members of the public who wish to fly small Unmanned Aircraft Systems (small UAS or sUAS) weighing less than 55 pounds in controlled airspace (Class B, Class C, Class D, or within the lateral boundaries of the surface area of Class E airspace designated for an airport) must request and receive prior authorization from the FAA prior to conducting the flight operations. These individuals are divided into two general groups: (1) limited recreational operators as described in 49 U.S.C. § 44809(a) and (2) sUAS operators as described in 14 C.F.R. part 107. This document covers anyone who wishes to fly a sUAS under either § 44809(a) or part 107.

The Federal Aviation Administration (FAA) developed the Low Altitude Authorization and Notification Capability (LAANC) to help process requests for authorizations. LAANC creates an automated way for individuals to conduct sUAS operations in controlled airspace. LAANC relies on a private-public partnership between the FAA and UAS Service Suppliers (USSs).

The Department of Transportation/FAA is updating the previously adjudicated Privacy Impact Assessment (PIA), which was published on the DOT website on October 15, 2018. This update reflects changes to the program resulting from the FAA Reauthorization Act of 2018, which enacted § 44809(a) requiring authorizations for limited recreational operators flying sUAS in controlled airspace. Before the enactment of § 44809(a), LAANC only allowed sUAS operators who operated under 14 C.F.R. Part 107 to submit requests for authorization, as limited recreational operators as defined under previous law were not required to receive authorizations before flying in controlled airspace. Now, both types of operators (Part 107 and § 44809(a)) are required to request and receive such authorizations. Amendments to this PIA clarify that information will be collected from those operating under § 44809(a).

This update will continue to inform the public of the privacy risks and mitigation strategies associated with the FAA's collection, use, dissemination, and retention of Personally identifiable Information (PII) resulting from LAANC.

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

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).

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

Individual members of the public who wish to fly sUAS weighing less than 55 lbs. (small UAS or sUAS) in controlled airspace (Class B, Class C, Class D, or within the lateral boundaries of the surface area of Class E airspace designated for an airport) must request and receive prior authorization from the FAA prior to conducting the flight operations. These individuals are divided into two general groups: (1) limited recreational operators as described in 49 U.S.C. § 44809(a) and (2) operators as described in 14 C.F.R. part 107. Throughout this document the term "sUAS operator" is intended to cover operators flying under either § 44809(a) or part 107.

Before the development of LAANC, the only way for sUAS operators to request these airspace authorizations was through a manual process. That process, which still exists, often entailed a waiting period of up to 90 days for approval of the authorization.

LAANC streamlines this process by automating the FAA's ability to grant airspace authorizations to sUAS operators. Using LAANC, a sUAS operator submits a request for airspace authorization to operate a sUAS to the FAA via an application on a computer or mobile device developed and run by a third party USS qualified by the FAA. The USS collects this information on behalf of the FAA regarding the date, time, and location of the proposed operation and processes the request to the FAA. The FAA responds to the sUAS operator through the USS, advising whether the request for authorization is approved or denied.

LAANC includes three main parties: sUAS operator, USS, and FAA.

sUAS Operator

sUAS operators must request authorization to operate in controlled airspace.² Using LAANC, a sUAS operator will be required to provide the following data, which the USS will collect (and then transfer) to the FAA: first name, last name, telephone number, and flight plan information.³ Flight plan information required for authorizations is the start date and time, duration, maximum altitude, airspace location, and UAS registration number (optional). The information listed in this paragraph is the only information that the FAA requires the USS to collect.

² Part 107 and § 44809 both establish that no person may operate a small unmanned aircraft in Class B, Class C, or Class D airspace or within the lateral boundaries of Class E airspace designated for an airport unless that person has prior authorization.

³ Information collected by LAANC in connection with authorization is collected in furtherance of maintaining safety in the NAS. See 49 U.S.C. §44809.

If the USS collects or requests any information from sUAS Operators that the FAA does not require, that information is not sent to the FAA. Each USS is required to enter into a Memorandum of Agreement (MOA) with the FAA.⁴ The MOA prohibits the USS from sending information to the FAA other than the required information listed above. Information collected by the USS for its own purposes is maintained and shared according to each USS's privacy policy. The FAA does not determine the USS's privacy policy. The MOA requires USSs to provide a privacy statement to users identifying which information is required by FAA and that any additional information collected by the USS is subject to the USS's own privacy policy. The FAA does not currently actively monitor the USSs, but this will change in 2019 and the FAA plans to begin active monitoring by the end of 2019. If a violation of the MOA or Operating Rules occurs, the FAA can revoke the USS's MOA.

In order to use LAANC, sUAS operators must use an FAA-qualified USS (see below section "UAS Service Supplier") through an application that is downloaded to the sUAS operator's computer system or mobile device. Any fees associated with using a USS's application is determined by the USS and the FAA is not involved with determining the costs. As of April 2019, no USSs are charging fees. sUAS operators are not required to use LAANC in order to request an airspace authorization. sUAS Operators can instead choose to contact the FAA directly to request authorization.⁵

UAS Service Supplier

USSs provide authorization communication services between sUAS operators and the FAA. USSs are industry partners of the FAA. The USSs are responsible for developing an application that sUAS operators can use to make authorization requests. The USSs will collect the above-described information to send to the FAA. The FAA will use this information to approve/deny authorization requests. Requests are approved or denied based solely upon the flight plan information and current NAS conditions.

The USSs communicate with the FAA through Application Programming Interfaces (API). The APIs are continuously tested, proven, controlled, and securely managed. USSs are also subject to Operating Rules⁶ and go through an onboarding process. Onboarding includes signing the MOA, proving that USSs can meet the Operating Rules, and testing the end-to-end system and connections.

The USSs will manage and store all the initial records for the sUAS operator. As described above, the USS will request and collect information from the sUAS operator to process the transaction. Security of the sUAS operator's information that is in the possession of the USS is the USS's responsibility. USSs are required to interact with LAANC API in accordance with information security requirements defined by NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.⁷ Also, the Operating Rules require the USSs to notify all sUAS operators using their service of the LAANC Privacy Statement.⁸ The Privacy Statement advises sUAS operators of their privacy rights, that the FAA does not require sUAS operators to provide additional information to

⁴ The MOA is found here:

https://www.faa.gov/uas/programs_partnerships/data_exchange/laanc_for_industry/media/FAA_LAANC_AP_MOA.pdf

⁵ This process can be completed by using FAA's "Drone Zone" portal, by visiting <https://faadronezone.faa.gov/#/>. DroneZone's PIA is published on DOT's website: <https://transportation.gov/privacy>.

⁶ Operating Rules are found here:

https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/industry/media/uss_operating_rules.pdf

⁷ See <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

⁸ The privacy statement is found at: https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/privacy_statement/

the USS, that airspace authorization requests can be sent directly to the FAA, and the security measures in place at the FAA to safeguard their information. See Transparency section below for greater detail on the Privacy Statement.

USSs are private entities and can be based either in the United States or in foreign countries. Therefore, it is possible that sUAS operators may encounter USSs that are not based in the USA. However, all USSs are required to conform to the same set of Operating Rules. Therefore, the privacy requirements and expectations are uniformly applied to all USSs regardless of where the USS is based. Additionally, sUAS operators are free to use any USS that they choose or are free to bypass USSs entirely and contact the FAA directly to make an authorization request.

FAA

FAA Air Traffic Managers (ATMs) may access the data once it is sent to the FAA. The FAA authorizes an ATM to access this data through a secure means after the ATM's identity is authenticated. The FAA will only receive and have access to the sUAS operator's information as described in the Introduction & System Overview section above. Any additional information the USS requests from the sUAS operator is not sent to the FAA. In rare emergency cases the FAA may reach out to the sUAS operator directly via the provided telephone number to make the operator aware of a cancelation or emergency.

The FAA owns the LAANC system. The USSs, if able to meet all the requirements described above, provide applications to sUAS operators to submit flight operations to LAANC. There is no financial relationship between the FAA and the USSs. Additionally, USSs are responsible for the design of their application. The FAA is not involved in the design of the applications other than to provide and test system requirements

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3⁹, 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.¹⁰

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.

⁹ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

¹⁰ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

As described above, the FAA collects information to process authorization requests. Through LAANC, the FAA collects the minimum amount of information necessary to provide these services. The FAA informs sUAS operators of the reason why the information is collected in a number of ways.

The FAA maintains and retrieves records in LAANC by the sUAS operator's name and telephone number. The FAA protects Privacy Act records in accordance DOT/FAA 854 "Small Unmanned Aircraft Systems Waivers and Authorizations" which provides notice to the public of FAA's privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information collected from sUAS operators related to waivers and authorizations.¹¹

The Operating Rules require the USSs to advise sUAS operators of the Privacy Act Statement as required under the Privacy Act, 5 U.S.C. § 552a(e)(3). The Privacy Act Statement covers LAANC's information collection in detail. The Privacy Act Statement advises the sUAS operator that the information collected for FAA purposes is pursuant to 49 U.S.C. § 44809(a) and Part 107, what information is required under the law, and what information is provided to the FAA. The Privacy Act Statement further advises sUAS operators that if the USS requests information beyond what the FAA requires that additional information is not provided to the FAA. Any additional information is protected and used in accordance with the USS's privacy policy and not the FAA's. The Privacy Act Statement also instructs sUAS operators that they are not required to use USSs and can submit authorization requests directly to the FAA. Finally, the Privacy Act Statement advises that all information sent to the FAA is protected, stored, used, and disclosed in accordance with SORN DOT/FAA 854. The Privacy Act Statement can be reviewed in its entirety at https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/privacy_statement/.

sUAS operators will have the opportunity to review and acknowledge any terms and conditions of using LAANC through their preferred USS provider. The FAA is not maintaining oversight over the USSs for any information the USSs request from sUAS operators beyond what the FAA requires. The relationship between the sUAS operators and the USSs outside of FAA-requirements belongs to those private parties and the FAA does not interfere with that relationship. No sUAS operator is required to use a USS to submit an authorization request to the FAA. Authorization requests can be submitted directly to the FAA at <https://faadronezone.faa.gov/#/>.

All requests submitted through LAANC are also subject to the requirements of the Paperwork Reduction Act (PRA). The Office of Management and Budget (OMB) has approved LAANC collecting information from Part 107 operators. LAANC's approval is covered under OMB Control Number 2120-0768. The FAA is in the process of requesting approval from OMB for collecting information from § 44809(a) operators. Information related to LAANC's status under the PRA is found at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201712-2120-002.

Finally, the publication of this PIA demonstrates FAA's commitment to provide appropriate transparency into its collection and maintenance of information through LAANC.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in

¹¹ See <https://www.gpo.gov/fdsys/pkg/FR-2016-08-02/pdf/2016-18208.pdf>. Although DOT/FAA 854 applies to requests for both waivers and authorizations, the LAANC system will not collect requests for waivers as described at 14 CFR § 107.200.

the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

sUAS operators are active and informed participants throughout the process of using LAANC. All use of LAANC is voluntary. However, if a sUAS operator chooses to use LAANC, the FAA-required information is necessary to determine if the sUAS operation can be done safely. USS providers may require information in addition to that required by the FAA. As discussed above, sUAS operators are free to use any USS and are free to base their decision on what information is collected. Although the manual process can be more time consuming, sUAS operators are also free to request the authorization directly from FAA rather than requesting them through LAANC using a USS.

The FAA and USSs inform the sUAS operator as to how the government will collect, use, and disclose the sUAS operator's Personally Identifiable Information (PII) each time the sUAS operator uses LAANC. The "Transparency" section details the Privacy Statement provided to sUAS operators so that they can make informed decisions regarding LAANC.

The sUAS operator is the source of all the information provided through the USS to the FAA. The sUAS operator has the opportunity throughout the process to review and make any changes to the information provided. No records are provided to the FAA unless the sUAS operator provides and submits the information. Any additional information that a USS may ask a sUAS operator to provide is beyond the reach of the FAA. The FAA does not interfere with this private relationship between the USSs and the sUAS operators.

Under the provisions of the Privacy Act, individuals may request searches of FAA records maintained in accordance with the DOT/FAA 854 SORN to determine if any records in the FAA LAANC system may pertain to them. If sUAS operators want to know about any additional data collected by their selected USS provider, they can reach out to USSs directly and/or review the USS's privacy policy.

Individuals wishing to know if their records appear in the FAA LAANC system or who have privacy concerns about the FAA LAANC system may inquire in person or in writing to:

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

The following information must be included in the written request:

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

Individuals expressing a complaint about the privacy practices of the FAA LAANC system should provide details of the situation or condition about which they are filing the complaint.

Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons why the records should be corrected 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 its collects, uses, maintains, or disseminates PII.

LAANC collects information from sUAS operators to receive and respond to requests for authorization to operate an sUAS in Class B, C, or D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport. The information that is collected by the FAA through the USS is the minimum amount necessary to comply with 49 U.S.C. § 44807 and maintain the safety of the NAS. Information collected by the USS is maintained by the USS in accordance with its own privacy policy. The MOA between the USS and FAA, and associated Operating Rules, contain requirements for the USS to have a privacy policy in place and to provide the Privacy Statement to users (discussed above). If a violation of the MOA or Operating Rules occurs, the FAA can revoke the USS's MOA.

The FAA may use the sUAS operator's contact information to provide information about potential unsafe conditions to sUAS owners and operators and to educate them regarding possible risks to their operation.

In addition to 14 C.F.R. § 107.41 and 49 U.S.C. § 44809(a), the following authorities authorize LAANC's information collection:

- 49 U.S.C. § 44807, Special Authority for Certain Unmanned Aircraft Systems,
- 49 U.S.C. § 106(f), Authority of the Secretary and the Administrator,
- 49 U.S.C. § 106(g), Duties and powers of Administrator,
- 49 U.S.C. § 40101, Policy,
- 49 U.S.C. § 40103, Sovereignty and use of airspace,
- 49 U.S.C. § 40106, Emergency powers,
- 49 U.S.C. § 40113, Administrative,
- 49 U.S.C. § 44701, General requirements,
- 49 U.S.C. § 44721, Aeronautical charts and related products and services, and
- 49 U.S.C. § 46308, Interference with air navigation.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The DOT is requesting the minimum amount of information necessary to meet its statutory requirements of maintaining safe airspace and introducing sUAS to the NAS. LAANC will collect and retain only the following information from sUAS operators: first name, last name, telephone number, and flight plan information (as

described in the Introduction & System Overview section). ATMs may use the contact information (name and phone number) to contact the sUAS operator to support NAS operations. For example, if there is an emergency situation that requires an immediate grounding of all sUAS operations, the ATM may want to contact the sUAS operators directly.

The FAA is currently seeking records disposition authority from the National Archives and Records Administration (NARA) for records related to authorizations as described below. Until that authority has been identified, these records will be retained indefinitely. LAANC is seeking to retain the records for a period of two years.

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.

PII collected by the FAA will be used only as specified in the Department's system of records notice DOT/FAA – 854, "Small Unmanned Aircraft Systems Waivers and Authorizations" which applies to records collected in connection with sUAS authorizations submitted via LAANC or directly to the FAA.

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 DOT/FAA-854 may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as provided in the system of notice record (SORN) that applies to those records.

1. To the public, waiver applications and decisions, including any history of previous, pending, existing, or denied requests for waivers applicable to the sUAS at issue for purposes of the waiver, and special provisions applicable to the sUAS operation that is the subject of the request. Email addresses and telephone numbers will not be disclosed pursuant to this Routine Use. Airspace authorizations the FAA issues also will 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. Disclose information to the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.
3. 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.
4. 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.
5. 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.

6. 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.
- 6b. 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 (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 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.
7. The information contained in this system of records will be disclosed to the Office of Management and Budget, OMB in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.
8. 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 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).
9. 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 USC 2904 and 2906.
10. DOT may make available to another agency or instrumentality of any government jurisdiction, including State and local governments, listings of names from any system of records in DOT for use in law enforcement activities, either civil or criminal, or to expose fraudulent claims, regardless of the stated purpose for the collection of the information in the system of records. These enforcement activities are generally referred to as matching programs because two lists of names are checked for match using automated assistance. This routine

use is advisory in nature and does not offer unrestricted access to systems of records for such law enforcement and related antifraud activities. Each request will be considered on the basis of its purpose, merits, cost effectiveness and alternatives using Instructions on reporting computer matching programs to the Office of Management and Budget, OMB, Congress and the public, published by the Director, OMB, dated September 20, 1989.

11. DOT may disclose records from this system, as a routine use to appropriate agencies, entities and persons when (1) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DOT has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DOT or another agency or entity) that rely upon the, compromised information; 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 compromise and prevent, minimize, or remedy such harm.
12. 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.
13. 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.
14. DOT may disclose records from this system, as a routine use, to an agency, organization, or individual for the purpose of performing audit or oversight operations related to this system of records, but only such records as are necessary and relevant to the audit or oversight activity. This routine use does not apply to intra-agency sharing authorized under Section (b) (1), of the Privacy Act.
15. 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).

As noted above, USSs may require information beyond what is required by the FAA. The FAA does not receive this additional information and, therefore, cannot share or disclose the information. As private entities, the USSs are not subject to the Privacy Act and SORN 854 in their maintenance and disclosure of information; the USSs' individual privacy policies govern how the PII and other data they collect and maintain for their own purposes is disclosed. As discussed earlier, all USSs entered into a MOA with the FAA. The MOA prohibits the USSs from providing any information or data to the FAA other than what the FAA requires (as described above in Introduction and System Overview Section of this PIA). The MOA does not otherwise limit the USS's use of the data.

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).

sUAS operators providing information to the FAA are responsible for ensuring the accuracy of their own data. The FAA does not collect nor is it provided any information other than what the sUAS operator supplies. Individuals will be completely aware of all information that the DOT possesses.

Only the sUAS operator through the USS will have the ability to input data in the PII fields. The data fields are coded so only alpha characters are allowed in name fields and numeric characters in phone number fields. Control is very carefully exercised and only those with credentialed access (which is extremely limited) are allowed access to the data beyond "read" ability. At the request of the sUAS operator the USS can change information previously submitted. No one else has access to make changes to the information. LAANC maintains a history of all data fields so if any changes are made to the data, there is a record of any change for full transparency.

Through LAANC, the FAA will provide no authorization requests unless it has received the complete information set needed to do so. All information collected and the manner in which it is used is contained in the DOT/FAA-854 SORN.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

FAA protects PII in its system with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

The FAA performed the necessary assessment on the LAANC system in all areas including architecture, capabilities, implemented security postures, and system configuration. Security risks and deficiencies were then analyzed. After any risks and deficiencies were addressed, LAANC received an "Authority To Operate". This process ensures that LAANC meets the necessary security standards and controls. The LAANC program will follow the System Impact Assessment process for any subsequent upgrade or enhancement efforts to ensure the LAANC system will stay secure. As described in the Information and System Overview Section, USSs are put through an onboarding test. During this testing, USSs must prove they can meet all LAANC security requirements as well as the Operating Rules. As stated above, security of the sUAS operator's information will be the USS's responsibility. All USSs are subject to a MOA which requires them to interact with LAANC API in accordance with information security requirements defined by NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. The MOA also requires that the USS send only the required records to the FAA.

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's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for governance and administration of FAA Order 1370.121, FAA Information Security and Privacy Program & Policy. FAA Order 1370.121 implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), FISMA, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

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

Responsible Official

Casey Nair,
LAANC Program Manager

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer