U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Commercial Space Transportation (AST)
Licensing Electronic Application Portal (LEAP)

Responsible Official

Michelle Murray
Email: michelle.murray@faa.gov
Phone Number: 202-267-1540

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Office of Commercial Space Transportation (AST) developed the Licensing Electronic Application Portal (LEAP) to enhance the efficiency of collecting and processing applications for commercial space licenses. LEAP enables the AST to automate the intake and processing of these applications. LEAP operates under 51 U.S.C. Chapter 509. Specifically, §5 0905 requires those participating in commercial space launch activities to apply for a license, demonstrating their operation is consistent with the public health and safety.

The FAA is publishing this Privacy Impact Assessment (PIA) for the LEAP system in accordance with Section 208 of the E-Government Act of 2002 because the system processes Personally Identifiable Information (PII) from members of the public involved in the commercial space license application process, including applicants representing commercial space companies and other government agencies such as the National Aeronautics and Space administration (NASA) and Department of Defense (DoD).

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 electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

[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).

- *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

Under 51 U.S.C. §50905, the DOT has the authority to regulate commercial space launch activities. Part of this, as defined in section §50905, is the requirement for those participating in commercial space launch activities to apply for a license, demonstrating that their operation is "consistent with the public health and safety, safety of property, and national security and foreign policy interest of the United States."[2] FAA AST is responsible for carrying out this requirement and does so through its license application process. To obtain a license, applicants must submit documentation to demonstrate compliance with AST's safety requirements including: (1) Flight Safety Analysis, (2) Ground Safety, (3) Mishap Plan, and (4) Human Space Flight procedures. It is the responsibility of AST to ensure safe operations and foster the growth of the commercial space industry, and making quality determinations faster to keep pace with the industry is a must to accomplish this. The LEAP system streamlines this process by providing a centralized web portal to enable the following:

- Applicants (the company submitting the license application is referred to as the "applicant") can submit their applications and track their status.
- AST can monitor open applications and provide prompt feedback to applicants.
- Stakeholders from other executive departments and agencies review applications and provide input needed to meet AST's interagency review requirement.[3]

FAA employees and contractors, government stakeholders from other US executive departments and agencies, and agents representing the companies applying for Commercial Space Launch and Reentry Licenses log in to LEAP using MyAccess for authentication at

[2] 51 U.S.C. § 50905(a) (2023)
[3] Exec. Order No. 12,465, *Coordination and Encouragement of Commercial Expendable Launch Vehicle Activities*, 49 Fed. Reg. 32,779 (Aug. 13, 1984)

the uniform resource locator (URL) leap.faa.gov. The PII collected includes email address, first name, and last name.

External users (non-Personal Identity Verification (PIV) or Common Access Card (CAC) holders) who are applicant agents and not credentialed, or federal users, request an account using the uniform resource locator (URL) Login.gov. The account is created using the requester's email address. The information collected by Login.gov includes email address, first name, and last name.

A typical transaction on the LEAP system looks like the following:

1. The applicant submits documentation related to their Commercial Launch or Reentry License application in electronic formats, such as Microsoft Word, PDF, and Excel, as well as non-human formats (e.g., trajectory files).
2. LEAP creates a task for AST's task management system to review the applicant's submission.
3. AST and the applicant iterate on submissions until all application requirements are met.

Some of the application data submitted in Step 1 is provided to other government stakeholders such as Flight Safety Analysis, Ground Safety plan, Mishap Plan, and Human Space Flight procedures, for input and feedback. AST can also engage directly with applicants on LEAP to answer questions they may have about their application.

The LEAP system collects and keeps two types of data that may include PII such as users' login details and application documents. The PII for logins includes email address, first name, and last name. The PII contained in application documents may contain full names, company addresses, work phone numbers, email addresses, International Traffic in Arms Regulation (ITAR) restricted data, and proprietary data.

AST officials can access Launch and Reentry application documents and applicant data for evaluation. Applicants receive official feedback from AST through LEAP. Outputs are tailored to recipients' need-to-know and access levels and are available to both Launch and Reentry License Applicants and AST officials.

Interagency partners have limited access to application materials to support the FAA's coordinated policy review of license applications under Part 450.31 (Policy review and approval). They can download, view, and comment on selected documents, and upload supporting documentation to the LEAP application. Interagency partners include a select group of non-FAA federal employees from the following agencies: DoD, NASA, National Oceanic and Atmospheric Administration (NOAA), Federal Communications Commission (FCC), US Coast Guard (USCG), US Space Force (USSF), Department of State (DOS), Department of Commerce (DOC), and National Geospatial-Intelligence Agency (NGA).

Applicants' information is not shared with other applicants. LEAP stores submitted documents in FAA Cloud Services (FCS) for review and archiving.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[4], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[5].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records, the existence of which is not known to the public.

The FAA employs multiple methods to ensure transparency in privacy practices. System of Records Notices (SORNs) inform individuals about collection, use, dissemination, and retention of PII within LEAP. LEAP provides a Privacy Act Statement explaining the purpose of information collection before any data is gathered. This PIA outlines LEAP's policies, procedures, and practices for information storage, data use, access, notification, retention, and disposal.

External users (non- PIV or CAC holders), including applicant agents who are not credentialed federal users) request an account using Login.gov. The account is created using the requester's email address. The external user goes to Login.gov, accepts the FAA Rules of Use, and is presented with the Privacy Act Statement (PAS). The PAS discusses the Department's privacy practices regarding collection, use, sharing, maintenance, and disposal of PII and appears at the initial point of collections.

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Access-related records about individuals who access LEAP are maintained in accordance with the Department's Privacy Act SORN, DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002), which cover authentication and access, maintain audit trails, monitor security for external users who use the LEAP system and collect information solely for its intended purpose to process commercial space license applications.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the LEAP system.

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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The applicant, who is an authorized representative of launch vehicle providers, enters the PII into LEAP and confirms that the information collected for the commercial space license application is true and accurate before submitting it.

Under the provisions of the Privacy Act, individuals may request searches of the LEAP system to determine if any records have been added that may pertain to them and if such records are accurate.

For all inquiries related to the information contained in the LEAP, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Federal Aviation Administration

Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

The request must include the following information:

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

If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

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.

Congress authorized the FAA Administrator to develop systems and/or tools to support the commercial space licensing process. LEAP addresses the unique demands of the FAA's workforce and operates under the authority of 51 U.S.C. §50905. This section describes the license application and requirements to participate in commercial space launch activities.

LEAP maintains PII on FAA employees, and government representatives of other US Government agencies, the Department of Defense, and agents representing the companies applying for Commercial Space Launch and Reentry Licenses to manage the LEAP program and for authentication and access. LEAP maintains first name, last name, and email address.

For external users, LEAP maintains the PII for authentication and access, which includes first name, last name, and email address.

The FAA uses this access information to create and validate login credentials, maintain audit trails, and monitor security for external users who use the LEAP system and FAA employees who use and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable system of records notice,

The FAA protects these records subject to the Privacy Act in accordance with the following Department's Published System of Records Notices (SORNs): DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 approved May 7, 2002.

The PII in the LEAP system is not routinely used for any other purposes.

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.

The FAA minimizes its data maintenance, use, and retention in LEAP to only the information that is relevant and necessary to meet its authorized business purpose of supporting the Commercial Space License application process.

The FAA keeps records from LEAP's License Application files and Compliance Monitoring Documents permanently. After these files are closed, the records are stored for 15 years before being sent to the National Archives for long-term preservation. N1-237-96-001

System access records are governed by the National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2, Information Systems

Security Records, approved in January 2023. Under that schedule, system access records are destroyed when business use ceases[6].

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The sharing of user account information in LEAP is conducted in accordance with SORN DOT/ALL 13, which pertains to Internet and Intranet Activity and Access Records (67 FR 30757, May 7, 2002). The FAA/DOT limits the scope of PII collected to what is necessary for authenticating external users within the system and ensuring that specific documentation submitted by applications for operations is properly managed.

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.
- To other government agencies where required by law.

Access and authentication records within LEAP are also handled in accordance with SORN DOT/ALL 13. Additionally, the Department has published 15 routine uses that apply to all DOT Privacy Act systems of records, including this one. These routine uses can be found in the Federal Register at 75 FR 82132 (December 29, 2010), 77 FR 42796 (July 20, 2012), and 84 FR 55222 (October 15, 2019).

The FAA does not use the PII for any other purpose.

[6] (NARA) General Records Schedule (GRS) 3.2, *Information Systems Security Records*, approved January 2023.

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).

The FAA retains the relevant and necessary information from authorized users[7] for LEAP's intended purpose of facilitating commercial space license applications. LEAP validates PII collected and maintained for system access through PIV, and PII collected for commercial space license applications are certified by applicants to be true and accurate before submission. The FAA coordinates with all external parties to ensure any PII collected and maintained in LEAP is associated with entities necessary to support LEAP's intended purpose at the point in time of collection.

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.

LEAP utilizes role-based access to ensure personnel are allowed the minimum access required to perform their assigned duties.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the LEAP system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in LEAP. All data in-transit is encrypted and access to electronic records is controlled by PIV and Personal Identification Number

[7] Authorized users are FAA employees and contractors, government representatives of other US Government agencies & the Department of Defense, and agents representing the companies applying for Commercial Space Launch and Reentry Licenses.

(PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessments to test and validate security process, procedures and posture of the system. Based on security testing and evaluation in accordance with the FISMA, the FAA issues LEAP an on-going authorization to operate (ATO).

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.

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures, especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with the LEAP portal are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of LEAP as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Michelle Murray
System Owner
Office of Commercial Space Transportation

Approval and Signature

Karyn Gorman
Chief Privacy Officer KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.05.27 12:07:54 -04'00'
Office of the Chief Digital & Information Officer