U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

FAA

National Airspace System Defense Programs

NDP

Responsible Official

Haris Velic
Email: haris.velic@faa.gov
Phone Number: 202-880-2993

Reviewing Official

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

Executive Summary

The National Airspace System (NAS) Defense Program (NDP) is a Federal Aviation Administration (FAA) system that provides the Department of Defense (DoD) and other National Security related groups with the necessary information to support their missions. NDP systems allow users/agencies to vet the propriety of an aircraft to occupy certain airspace, apply for permission to overfly a restricted area (waiver), alert to unauthorized incursions, detect flight plan variations, and identify suspicious/missing/stolen aircraft. NDP consists of eleven subsystems; however, this Privacy Impact Assessment (PIA) discusses only the Airspace Access Program (AAP) system and the Airspace Awareness and Detection System (AADS).

The FAA owns the AAP system and provides a method for individuals to submit requests for waivers to fly aircraft within restricted airspace. The management of the waivers is a joint effort of FAA and the Transportation Security Administration (TSA) for safeguarding American airspace. The FAA manages the safety requirements for aircraft operators seeking to operate in restricted airspace, while the TSA manages the security requirements.

AADS is a website accessible to National Security Agencies that consumes publicly available data from various systems and also includes Aircraft Registry and TSA data. AADS then correlates the various source data with aircraft positional track data to provide a complete situational awareness of that aircraft, its owner, its operator, and any other available attributes.

It was determined that waiver letters maintained by the FAA are not retrieved by an identifier but by the event and are not subject to the Privacy Act. The FAA is updating the PIA, in accordance with Section 208 of the E-Government Act of 2002, to remove DOT/FAA 801, Aviation 81 FR 54187 – August 15, 2016 (since updated and republished as DOT/FAA 801 Aviation Registration Records). Additionally, the record retention schedule was approved since the previously published PIA. The AAP system collects the aircraft operator's and aircraft owner's name, organization/company, address, phone number, and email address. For individuals traveling aboard the aircraft, the AAP system collects the individual's name, gender, date of birth, Social Security number, passport number, and country of issuance, city of birth, pilot certificate number, and pilot certificate country. AADS also collects aircraft ownership information, including the aircraft owner's name, address, and phone number.

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:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Federal Aviation Act of 1958 gives the FAA the responsibility to implement safety programs to ensure the world's safest, most efficient aerospace system. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

[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).

NDP is a post 9/11 FAA program established to provide advanced flight plan data, surveillance data, communications capabilities, and emerging services to support the National Security Departments, their agencies, and their missions. NDP utilizes existing federal infrastructure and human resources to expand voice, flight data, and surveillance services to meet external requirements. NDP evaluates current and planned federal assets, plans, policies, and procedures for applications in developing and sustaining national air security capability.

Airspace Access Program

TSA is a component of the Department of Homeland Security (DHS) and is responsible for the security of the nation's transportation systems. TSA's mission is to protect the nation's transportation systems by ensuring freedom of movement for people and commerce. The FAA is responsible for civil aviation safety. Safe and efficient use of navigable airspace is a primary objective of the FAA. The agency operates a network of airport towers, air route traffic control centers, and flight service stations. The FAA also develops air traffic rules, assigns airspace use, and controls air traffic. The AAP system is a joint effort of the FAA and TSA for safeguarding American Airspace and provides a method for individuals to submit requests for waivers to fly aircraft within restricted airspace.

The AAP system is designed to provide public users with an easily accessible, user-friendly online application for submitting and tracking waiver requests. The system allows for submissions and tracking in the following categories:

- Unmanned Aircraft Waivers
- Sporting Event Waivers
- Special Event Waivers
- Moored Balloon Waivers
- International Waivers
- Domestic Waivers
- Disney Theme Park (Florida and California) Waivers
- DCA Access Standard Security Program (DASSP) Authorization Waivers

To start the process of applying for a domestic and international waiver, the requester navigates to https://waivers.faa.gov. The requester must first create a user account and provide their name, title, user name, challenge question and answer, desk and mobile phone number, fax number, primary and secondary email address, and work address. The requester then manually enters their name as well as the, aircraft operator's and aircraft owner's names, organization/company, address, phone number, and email address. In addition, the requester enters information about individuals traveling aboard the aircraft, including their names, sexes, dates of birth, social security numbers, passport numbers and countries of issuance, cities of birth, pilot certificate numbers, and pilot certificate countries. The TSA collects all the information submitted as part of the waiver process to conduct a background check. The

TSA published a PIA titled *Airspace Waivers and Flight Authorizations for Certain Aviation Operations* that is available at https://www.dhs.gov/sites/default/files/publications/privacy_pia_tsaairspaceamend.pdf. Please see that PIA for a full discussion on the process for applying for a waiver.

Once TSA completes its background check, TSA forwards the request to the FAA for their review and approval or denial. After FAA review, if the waiver request comports with applicable safety requirements, FAA approves and signs the waiver request. If applicable safety requirements are not met, the FAA denies the waiver request. In both instances, the requester receives an email notification and can access the AAP system to download a PDF copy of the waiver request letter of approval/denial. For approval, the requester utilizes the approved waiver request during their flight. If a waiver is disapproved, the requester is not allowed to fly in the restricted airspace. The letter includes the requester's name, address, phone number, authorization number, and information submitted with the request.

Airspace Awareness and Detection System (AADS)

AADS is a real-time tracking system that combines publicly available data and unfiltered positional flight data (Sensitive Flight Data) from FAA systems that are consolidated and made available to Government agencies where its missions are rooted in national security and protection. Government users with approved accounts (FAA, TSA, DoD, DHS, etc.) are given AADS access to the AADS website at https://aads.faa.gov and log in with their username and password. Once logged in, users can select an aircraft track to view the aircraft's real-time position. Various databases, such as FAA Aircraft Registry, En Route Automation Modernization, Data Distribution System, NAS Message Rehost, Air Movement Information System, Operational Supportability Implementation System, and System Wide Information Management and additional systems are then correlated with that aircraft's positional track to provide the operator a complete situational awareness of that aircraft, its owner, and its operator. Typically, AADS users will query the aircraft's position on their screen to determine friendly versus foe and authorized or unauthorized aircraft. The system also provides the aircraft's ownership information (name, address, and phone number) during that inquiry.

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[2]*, 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*[3]*.*

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 AAP system is a joint effort of FAA and TSA to safeguard American airspace and provides a method for individuals to submit requests for waivers to fly aircraft within restricted airspace. FAA manages the AAP system website; however, TSA collects the required information to conduct security threat assessments. TSA provides notice via a Privacy Act Statement on the website to requesters of TSA's use of the information. In addition, TSA published System Record Notice DHS/TSA 002, Transportation Security Threat Assessment System, on August 11, 2014, 79 FR 46862, and PIA titled Airspace Waivers and Flight Authorizations for Certain Aviation Operations as a means of notice. The FAA approves the waiver requests. Those records are retrieved by the event number rather than an identifier. Therefore, the approved or denied waiver requests are not kept in a Privacy Act System of Records.

AADS collects and maintains information from publicly available sources. The only PII collected and maintained is the aircraft owner's name, address, and phone number. FAA provides notice of its use of this information on the Aircraft Registration System, which is the initial collection point. See the Aircraft Registration PIA available at https://www.transportation.gov/resources/individuals/privacy/aircraft-registration-system for a full discussion. AADS records are not about an individual and therefore they are not part of a Privacy Act System of Records.

The FAA collects users' names, titles, usernames, challenge questions and answers, desk and mobile phone numbers, fax numbers, primary and secondary email addresses, and work addresses for system access. The FAA retrieves system access records in the AAP system by name and other identifiers and protects these Privacy Act records in accordance with

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

Department's published SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30757.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency about its privacy practices to those who use NDP.

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.

The FAA manages the AAP system's website; however, TSA collects the required information to conduct security threat assessments. While creating the waiver, the requester can make a change to their waiver request. Once the waiver is submitted to TSA, the requester can withdraw their submission if changes are required. Lastly, once a waiver is approved, the requester can modify their request. Neither AAP nor AADS is a Privacy Act System of Records; therefore, they are not afforded provisions under the Privacy Act.

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.

TSA collects the requester's, aircraft operator's, and aircraft owner's names, organization/company, address, phone number, and email address. In addition, it collects the name, sex, date of birth, social security number, passport number, and country of issuance, and the city of birth of all individuals traveling aboard the aircraft; the pilot's certificate number and the pilot certificate country information are collected as well. The authority for TSA to collect the information is 49 U.S.C. § 114; Pub. L. 108-176, and the information is used by TSA to conduct security threat assessments.
AADS consumes data from public, non-public, and commercial resources as well as the following FAA systems: AVS Registry, En Route Automation Modernization, Data Distribution System, NAS Message Rehost, Air Movement Information System, Operational Supportability Implementation System, and System Wide Information Management. The unfiltered positional flight data (Sensitive Flight Data) is consolidated and made available to Government agencies whose missions are rooted in national security and protection. The only PII available to AADS users is publicly available data (FAA Registry), namely, the aircraft owner's name, address, and phone number. The authority for the FAA to collect this information is the Federal Aviation Act of 1958, as amended.

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 minimum amount of information is collected by TSA and managed by the FAA to process a waiver request. The FAA maintains records in accordance with DAA-0237-2022-0004, Airspace Access Program (AAP) System, which was approved in February 2023. Records are cutoff upon expiration of the waiver and then destroyed 10 years after the cutoff date.

Use Limitation

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

The FAA shares consolidated, unfiltered positional flight data (Sensitive Flight Data) it receives from its systems with Government agencies whose missions are rooted in national security and protection. The only PII that is shared from the publicly available source is the aircraft owner's name, address, and phone number. Primary records in the system are not Privacy Act Systems of Records.

The sharing of user account information in the AAP system is conducted in accordance with Department of Transportation SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30758. In addition to other disclosures generally permitted under 5 U.S.C. §552(a)(b) of the Privacy Act, all or a portion of the records or information contained in the system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C § 552a(b)(3) as follows:

- 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.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR

82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses" (available at http://www.transportation.gov/privacy).

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).

While creating the waiver, the requester can save it as a draft for further revisions before submitting it. Once the waiver is submitted to TSA, the requester can withdraw their submission if changes are required. In addition, once a waiver is approved, the requester can modify their request. The request is automatically flagged as a modification. While the modification request is processing, the original waiver request remains active; once the request is fully approved, it automatically supersedes the original one.

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.

The FAA protects PII through 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) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, dated September 2020.

The NPD system has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. NDP was granted its ATO on May 19, 2023, after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). FAA Security Personnel audit the NDP system to ensure FISMA compliance through an annual assessment according to NIST standards and guidance.

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.

The FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division, is responsible for governance and administration of FAA Order 1370-121B, FAA Information Security and Privacy Program and Policy. FAA Order 1370-121B implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-3470, the Federal Information Security Management Act (FISMA), Department of Transportation (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, additional policies and procedures will be consistently applied, especially as they relate to the 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 securing privacy data. Guidance is provided through mandatory annual security and privacy awareness training and the FAA Privacy Rules of Behavior. The DOT Privacy Office and the FAA Security Compliance Division (AIS-200) will conduct periodic privacy compliance reviews of NDP with the requirements of OMB Circular A-130.

Responsible Official

Haris Velic
System Owner
NDP Flight Data Program Manager, ATO AJO

Prepared by: Essie L. Bell, Acting FAA 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: 2026.05.01 10:52:44 -04'00'