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
Acting, Chief Privacy & Information Asset 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 allows 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 will only discuss 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 who apply to operate in restricted airspace, while the TSA manages the security requirements.

AADS is a website accessible to National Security Agencies that consumes publically 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 attributes available.

The FAA is developing a Privacy Impact Assessment (PIA), in accordance with Section 208 of the E-Government Act of 2002, because the AAP system collects the aircraft operator and aircraft owner's name, organization/company, address, phone number, and email address. In addition, for individuals traveling aboard the aircraft, that 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. Additionally, AADS collects aircraft ownership information including 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)

DOT Privacy Office - Approved - 08 03 2012

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 carry out safety programs to ensure the safest, most efficient aerospace system in the world. 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.

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, agencies, and their missions. NDP utilizes existing federal

[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).

DOT Privacy Office Approved - 08/03/2022

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 security of the nation's transportation systems. TSA's mission is to protect the nation's transportation systems by ensuring the 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 the use of airspace, and controls air traffic. The AAP system is a joint effort of FAA and TSA for safeguarding American Airspace and provides a method for individuals to submit requests for waivers to fly aircraft within restricted airspace.

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 the requesters, aircraft operator and aircraft owner's name, organization/company, address, phone number, and email address. In addition, the requester enters information of individuals traveling aboard the aircraft, including name, gender, date of birth, social security number, passport number and country of issuance, city of birth, pilot certificate number, and pilot certificate country. The TSA collects all information 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.

DOT Privacy Office - Approved - 08/03/2022

Once TSA completes its background check, TSA forwards the request to 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 meet, 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 from 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 via the https://aads.faa.gov and login with their username and password. Once logged on, the users can select an aircraft track to obtain a real-time position of the aircraft. 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 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 position in question on their screen to determine friendly versus foe and authorized or unauthorized aircraft. The system also provides the aircraft ownership information (name, address, and phone number) during that inquiry.

DOT Privacy Office Approved 02 03 2022

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].

[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

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, August 11, 2014, 79 FR 46862 and PIA titled Airspace Waivers and Flight Authorizations for Certain Aviation Operations as a means of notice.

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 at Aircraft Registration System, which is the initial collection point. See the Aircraft Registration PIA available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessment-faa-office-aviation-safety-aircraft-registration for a full discussion.

The FAA approves waiver requests in the AAP system that are retrieved by name and other identifiers and protects Privacy Act records in accordance with the Department's published System of Records Notice (SORN) covered by DOT/FAA 801, *Aircraft Registration System* 81 FR 54187 – August 15, 2016. AADS records are not about an individual and therefore not a Privacy Act System of Records. The FAA collects the name, title, username, challenge question and answer, desk and mobile phone number, fax number, primary and secondary email address, and work address for system access. The FAA retrieves system access records in AAP system by name and other identifiers and protects Privacy Act records in accordance with Department 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 provide 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.

DOT Privacy Office - Approved 08/05/2022

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.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington DC 20591

Included in the request must be the following:

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

Contesting record procedures:

Individuals wanting to contest information about themselves that is contained in AAP system should make their requests in writing, detailing the reasons for why their records should be corrected, to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington, DC 20591

DOT Privacy Office - Approved - 08 03 2022

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, aircraft operator and aircraft owner's name, organization/company, address, phone number, and email address. In addition, it collects the name, gender, date of birth, social security number, passport number and country of issuance, city of birth, pilot's certificate number, and pilot certificate country of all individuals traveling aboard the aircraft. The authority for TSA to collect the information is

49 U.S.C. § 114; Pub. L. 108-176 and the information will be used by TSA to conduct security threat assessments.

AADS consumes data from public, non-public, commercial, and 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 that is made available to the AADS user is the publicly available data (FAA Registry) the aircraft owner's name, address, and phone number. The authority for 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 has submitted a new records retention and disposition schedule DAA-0237-2022-0004 to the National Archives and Records Administration (NARA) in which it proposes to maintain the waiver request records for 10 years. The FAA will retain records in this system of records as permanent records until it receives approval of record disposition authority from NARA.

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), that it receives from the FAA 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.

The FAA maintains the approved waiver in accordance with Department published a System of Records Notice (SORN) DOT/FAA 801, Aircraft Registration System 81 FR 54187 – August 15, 2016. 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:

DOT Privacy Office - Approved - 08 03 2022

- To the public (including government entities, title companies, financial institutions, international organizations, FAA designee airworthiness inspectors, and others) information through the Aircraft Registry, including aircraft owner's name, address, United States Registration Number, aircraft type, and legal documents related to title or financing; and
- To law enforcement when necessary and relevant to a FAA enforcement activity.

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 make a change to their waiver request. 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 will automatically be flagged as a modification and while the modification request is processing, the original waiver request remains active, however, once the request is fully approved, it will automatically supersede the original one.

DOT Privacy Office- Approved- 08 03 2021

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 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) 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 March 3, 2022, 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 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 Privacy Office and the FAA Security Compliance Division (AIS-200) will conduct

DOT Privacy Office - Approved - 08/09/2022

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: Barbara Stance, FAA Privacy Officer

Approval and Signature

Karyn Gorman
Acting, Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

DOT Privacy Office - Approved - 08 03 2022

DOT Privacy Office - Approved - 08 03 2022