U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

FAA

Unmanned Aircraft Flight Restrictions Utility

UAFR-Utility

Responsible Official

Andrew Shutt
Email: Andrew.C.Shutt@faa.gov
Phone Number: (817) 913-9636

Reviewing Official

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

Executive Summary

The Unmanned Aircraft Flight Restriction Utility (UAFR-Utility) and Security Assessment Tool (SAT) is a Federal Aviation Administration (FAA) system co-led by the Air Traffic Organization (ATO) Enterprise Unmanned Aircraft System (UAS) Services program office (AJM-337) and the Office of Security and Hazardous Materials (ASH) UAS Program Design and Analytics Division (ASH-300). The UAFR-Utility and SAT is a new system currently in development, with an expected Authority to Operate (ATO) by the end of Q4 of Fiscal Year (FY) 2026.

The UAFR-Utility is an interactive, end-to-end solution for the management of Unmanned Aircraft Flight Restrictions (UAFRs), in accordance with procedures stated in the regulatory text of Title 14 of the Code of Federal Regulations (14 CFR) Part 74, *Designation of Unmanned Aircraft Flight Restrictions* – which is in the rulemaking process, with a Notice of Proposed Rulemaking (NPRM) scheduled to publish in Q2 of FY2026. The UAFR-Utility fulfills Part 74 requirements by providing a cloud-based web portal to designate UAFRs for eligible fixed site facilities.

The FAA is publishing this Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 for the UAFR-Utility because the system collects basic personal identifiers from members of the public, including *UAFR Authorized Users*, *UAFR UAS Operators*, and *UAFR Public Members* who choose to participate in the public comment process for the rulemaking.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle 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

UAFRs are airspace volumes designated under Part 74 where no person may operate an unmanned aircraft (UA), unless the operations fall within one of the exceptions stipulated in that rulemaking. Per Part 74, UAFRs may be established to restrict UA operations over eligible fixed site facilities specifically the 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government services and facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater. in the interest of aviation safety, public safety, national security, and homeland security.

The UAFR-Utility is linked to the SAT, which is an interactive solution for specialists from FAA/ASH and other Federal government Sector Risk Management Agencies (SRMAs) to conduct security reviews, in accordance with the procedures stated in the regulatory text of 14 CFR Part 74. The SAT provides a separate, secure interface for security and critical infrastructure specialists to access the UAFR-Utility, with the additional provision of Protected Critical Infrastructure Information (PCII), for use in the management of UAFRs.[2]

There are three categories of UAFR-U users:

UAFR Authorized Users are individuals eligible to apply for the designation of a UAFR, and those responsible for the designated UAFR. This user type specifically includes fixed site facility operators or proprietors, their designated representatives, and site managers.

[2] For initial deployment, the SAT will have its own CSAM ID. Eventually, both the UAFR-Utility and the SAT will be under a single security boundary with a single CSAM ID.

UAFR Public Members are individuals or organizations that choose to participate in the Public Notice and Comment process for conditionally approved UAFRs. This user type includes various parties who may be interested in the UAFR, including local residents, business owners, and UAS operators.

UAFR UAS Operators are organizations or individuals that are eligible to conduct allowed UAS operations[3] within effective, designated UAFRs. This user type specifically includes UAS operators from allowed organizations or other representatives of those organizations acting on their behalf.

The UAFR-Utility facilitates nine (9) typical transactions related to UAFR designation. Those transactions are described below, along with details about the collected and retrievable personal identifiers involved with each.[4]

System Functionality: Eligibility Determination (Transaction #1)

The operator or proprietor of a fixed site facility may submit an electronic request for Eligibility Determination – during which *FAA Processors* from the ATO, ASH and SRMA evaluate whether the fixed site facility is eligible for a UAFR designation, in accordance with specific criteria[5] outlined in Part 74, providing the requisite information to the FAA via the UAFR-Utility. The operator or proprietor must provide names and contact information for individuals associated with the UAFR request, along with the following information about the fixed site facility: facility name, physical address, website, sector, sector criteria justification, and UAFR request details including lateral boundaries (latitude/longitude), altitude ceiling (AGL), and activation duration (continuous or part-time) and schedule (if part-time). FAA Processors from ASH and SRMA access the UAFR-Utility via the SAT, leveraging UAFR data and additional PCII data to make UAFR determinations. UAFR Authorized Users provide this information through the UAFR-Utility, without the submittal of separate or additional forms outside system parameters.

Upon review, if the fixed site facility is deemed eligible to apply for a UAFR, the FAA provides Conditional Approval to the *UAFR Authorized User* along with an associated Tracking ID.

Basic personal identifiers about *UAFR Authorized Users* (name and contact information) are collected during this transaction. This data is maintained on the FAA cloud and accessible

[3] Per part 74, allowed operations within a UAFR are strictly limited to unmanned aircraft that (1) broadcast remote identification in accordance with 14 CFR part 89, (2) exit the UAFR as quickly as practicable, (3) are operated under one of the specified regulatory frameworks (14 CFR parts 91, 107, proposed 108, 135, or 137), and (4) are within a UAFR established under § 74.5.

[4] Certain transactions involve automated electronic requests for information from and/or about UAFR-Utility users. Data related to these transactions is created, maintained, and stored entirely within the UAFR-Utility. system. The system does not create "forms" or documents from the submitted data. Once submitted, the data is not retrievable by Members of the Public via access to the system.

[5] The eligibility criteria for each specific type of fixed site facility in subpart C of Part 74.

only via the UAFR-Utility. *FAA Processors* cannot retrieve UAFR records using personal identifiers provided during this transaction when performing queries using the UAFR-Utility.

System Functionality: Public Notice and Comment (Transaction #2)

When evaluating airspace restrictions of any type, the FAA seeks public input to assess the potential impact of the restriction and implement mitigations to minimize impact on the public's right to transit or on aviation operations. The UAFR public comment process is managed within the public UAFR-Utility website.[6] Interested parties can view Conditionally Approved UAFRs, submit comments on those UAFRs, and review others' posted comments and any responses provided by respective *UAFR Authorized Users* or *FAA Processors* – all publicly available within the UAFR-Utility.

To submit a comment, *UAFR Public Members* are required to establish a UAFR-Utility user account, which requires them to provide basic personal identifiers (name and email address) and create a password. Via their user accounts, *UAFR Public Members* may submit comments (1) anonymously (no name publicly posted with the comment), (2) as an individual (personal name publicly posted with the comment), or (3) on behalf of an organization (respective organization's name publicly posted with the comment). Commenters' email addresses are never publicly posted with comments. If their comments receive responses, commenters will receive automated, fixed response notifications from the UAFR-Utility system via in-system messages and emails.

The UAFR-Utility public comment web page includes a free-form text field in which comments can be written. A disclaimer alerts *UAFR Public Members* that comments will be available for examination on the UAFR-Utility before and after the comment closing date, and that personal identifiers (e.g., name, address, phone number) must not be submitted in the comment field because they will be disclosed with the comment via the internet.

In sum, basic personal identifiers about *UAFR Public Members* (name and contact information) are collected during user account creation. All public comments and personal identifiers provided to create a user account are stored on the FAA cloud. UAFR-Utility users cannot retrieve comment records using personal identifiers when querying the UAFR-Utility. Comments can only be queried using the Tracking ID and other information provided about the fixed site facility itself.

System Functionality: Application (Transaction #3)

Once the public comment period is closed, the operator or proprietor, or their designated representative, may prepare and submit a UAFR application. Per Part 74, the *UAFR*

[6] The UAFR public comment process emulates the process defined by the eRulemaking Program administered by the General Services Administration (GSA) via Regulations.gov, which enables the public to participate and impact Federal rules and regulations.

Authorized User must provide the FAA with a summary of the public comments received on the requested UAFR along with their proposed responses to those comments. The application includes submitting these materials to the FAA, along with the materials submitted to receive conditional approval and any adjustments to those materials. The FAA must evaluate the application to determine whether to grant the UAFR request within 90-days of receiving the application. The FAA then issues an Approval or Denial on the request to the *UAFR Authorized User*.

This transaction does not involve any additional collection of or retrieval using personal identifiers. All application data is stored on the FAA cloud. *UAFR Authorized Users* (while reviewing/responding to comments and preparing applications) and *FAA Processors* (while evaluating applications) can only query the UAFR-Utility using Tracking ID and other information provided about the fixed site facility itself.

System Functionality: Petition for Reconsideration (Transaction #4*)*

Upon Denial during Eligibility Determination or Denial of an Application, *UAFR Authorized Users* are provided an opportunity to petition for reconsideration of the FAA's denial via the UAFR-Utility. *UAFR Authorized Users* must demonstrate that (a) a material fact exists which was not previously presented to the FAA; (b) the FAA made a material error of fact; and/or (c) the FAA did not correctly interpret a law, regulation, or precedent.

FAA Processors then evaluate the petition and determine if it is valid. If valid, *FAA Processors* review the submittal again and may reverse or affirm its Denial. If invalid, *FAA Processors* affirm its denial. The *UAFR Authorized User* is notified via the UAFR-Utility in all cases. If the petition is in response to an Application Denial, the petition decision is also made available to the public.

This transaction does not involve any additional collection of, or retrieval, using personal identifiers. The petition and response are between the *UAFR Authorized User* and the *FAA Processor*, and all related data is stored on the FAA cloud. *FAA Processors* evaluating petitions can only query the UAFR-Utility using Tracking ID and other information provided about the fixed site facility itself.

System Functionality: Publication (Transaction #5)

All designated UAFRs are published and maintained on the UAFR-Utility. In addition, all UAFRs are published in the Federal Register, UAS Data Delivery Service (UDDS), and FAA Order Joint Order (JO) 7400.12,[7] *Unmanned Aircraft Flight Restriction Designations*, including status as approved, expired, or cancelled, as well as the following information: UAFR Site Identification Number (Site ID) assigned with Approval; organization associated

[7] Once part 74 has been finalized, an electronic version of JO 7400.12 will be available on FAA's website at https://www.faa.gov/air_traffic/publications/.

with the fixed site facility; city and state; lateral boundaries; altitude ceiling, activation duration and schedule (only if part-time), effective date, and expiration date.

This transaction does not involve any additional collection of or retrieval using personal identifiers. All UAFR data is stored on the FAA cloud and referenced for updates to the Federal Register, UDDS, and FAA JO 7400.12.

System Functionality: Amendment (Transaction #6)

After Publication, *UAFR Authorized Users* may determine that amendments to designated UAFRs are required – a process managed within the UAFR-Utility. Major amendments (i.e., increase in dimensions or activation duration) require *UAFR Authorized Users* to submit an amended Eligibility Determination and effectively repeat the UAFR request and approval process. Minor amendments (i.e., information updates related to the fixed site facility, operator, or proprietor, etc.) may be provided by *UAFR Authorized Users* themselves or upon request from *FAA Processors* and submitted directly in the UAFR-Utility as updates to the UAFR profile. Minor amendments that impact information contained in the Federal Register, UDDS, and FAA JO 7400.12 require repetition of the Publication process. Minor amendments that impact metadata require republication of the amended UAFR map in the UAFR-Utility.

Basic personal identifiers about *UAFR Authorized Users* (e.g., updated names and contact information) may be collected for minor UAFR amendments. This data is stored on the FAA cloud and accessible only via the UAFR-Utility. For Eligibility Determination, *FAA Processors* cannot retrieve records using personal identifiers provided during this transaction when querying the UAFR-Utility.

System Functionality: Renewal (Transaction #7)

No later than 120 days prior to the UAFR expiration date, *UAFR Authorized Users* receive a message within the UAFR-Utility and an associated email notification indicating that they may complete renewal requests in the UAFR-Utility. *FAA Processors* then evaluate those renewal requests and issue approval or denial determinations. When the UAFR expiration date passes, the UAFR-Utility notifies the *UAFR Authorized User* of the expired UAFR.

This transaction does not involve any additional collection of or retrieval using personal identifiers. *FAA Processors* reviewing renewal applications can only query the UAFR-Utility using Tracking ID and other information provided about the fixed site facility itself.

System Functionality: Cancellation (Transaction #8)

As appropriate, *UAFR Authorized Users* may directly submit UAFR cancellation requests via the UAFR-Utility, which take effect after confirmation by *FAA Processors*. Alternatively, *FAA Processors* may also issue proposed cancellations via the UAFR-Utility, which issues Proposed Cancellation Letters to *UAFR Authorized Users.*

This transaction does not involve any additional collection of personal identifiers. *FAA Processors* reviewing cancellations can only query the UAFR-Utility using Tracking ID and other information provided about the fixed site facility itself.

System Functionality: Access Notice (Transaction #9)

Per Part 74, allowed operations within a UAFR are strictly limited to unmanned aircraft that (1) broadcast remote identification in accordance with 14 CFR part 89, (2) exit the UAFR as quickly as practicable, (3) are operated under one of the specified regulatory frameworks (14 CFR parts 91, 107, proposed 108, 135, or 137), and (4) are within a UAFR established under § 74.5. These constraints both limit the categories of operators and require remote identification broadcasts that disclose aircraft identification and position-related data—factors that directly affect the nature and scope of personal and operational information processed during UAFR operations. When accessing a UAFR, *UAFR UAS Operators* must provide situational awareness to the respective fixed site facility contacts and the FAA as soon as reasonably possible by providing access notification via the UAFR-Utility. When time is insufficient to submit the access notification in advance of the operation, the *UAFR UAS Operator* may verbally notify a *UAFR Authorized User* associated with the UAFR of interest as soon as reasonably possible, then submit an access notification within seven days of the verbal notification.

Part 74 does permit *UAFR UAS Operators* to request non-routine access to a UAFR for operations that are not allowed. Such operators must have a UAFR-Utility user account and submit an access notification no less than 10 calendar days in advance of the operation, indicating their request to operate within the UAFR. *FAA Processors* then coordinate with and notify the respective *UAFR Authorized User*, review the planned operation, verify that the operator is not a security threat, and notify the requesting *UAFR UAS Operator* of approval or denial via the UAFR-Utility.

The access notification requires allowed UAS operations category; information about the person submitting the waiver request, providing the notification for the *UAFR UAS Operator* (name, mailing address, telephone number, and email address); the Site ID; and information about the proposed or actual operation (date, time, flight path, quantity of UA, UA registration number, and name and telephone number of the person in command of the UA). After submitting the data, *UAFR Authorized Users* and *FAA Processors* are notified by and may correspond with the *UAFR UAS Operator* via the UAFR-Utility.

Basic personal identifiers about *UAFR UAS Operators* (name and contact information) are collected during this transaction. This data is stored on the FAA cloud and accessible only via the UAFR-Utility. *FAA Processors* and *UAFR Authorized Users* reviewing and responding to access notifications, can only query the UAFR-Utility using Site ID and other information provided about the fixed site facility itself.

Reports

The UAFR-Utility supports two types of reports: (1) Unauthorized Access Reports, and (2) Annual Reports. This section details those outputs, along with the data contained in each and their respective users and viewers.

- ***Unauthorized Access Reporting:*** The *UAFR Authorized User* must document any cases of an unauthorized UAS operation in a designated UAFR by preparing and submitting an Unauthorized Access Report to the FAA via the UAFR-Utility. Depending upon what is known about the incident, this report can include location, timing, and other details about the operation, as well as details about the UA involved and UAS operator (mailing address, telephone number, and FAA-issued Airmen Certificate Number). *FAA Processors* can retrieve Unauthorized Access Report data by querying the UAFR-Utility by Site ID number, fixed site facility name, city, or state.
- ***Annual Reporting:*** The *UAFR Authorized User* is required to track the total number of UAS operations – both allowed and unauthorized – within a respective UAFR and submit a report on an annual basis to the FAA via the UAFR-Utility. This report includes the total number of operations and all Unauthorized Access Reports from that annual period.

Basic personal identifiers about unauthorized UAS operators may be contained in these reports, if known by the UAFR Authorized User. This data is stored on the FAA cloud and accessible only via the UAFR-Utility and is not publicly available. *FAA Processors* reviewing Unauthorized Access Reports can only query the UAFR-Utility using Site ID and other information provided about the fixed site facility itself. *UAFR Authorized Users* can only view those reports that have been previously submitted. Annual Reports do not contain any personal identifiers that may have been provided by *UAFR Authorized Users* about unauthorized *UAS Operators*.

Audit Logs

The UAFR-Utility must maintain an audit trail for each UAFR, which provides a complete chronological history of case file data transactions and updates made to UAFR geospatial data. Each case file record includes the UAFR Tracking ID or Site ID and the username of the *UAFR Authorized User* who submits a new case file or makes a change to case file data. Audit logs do not involve any additional collection of or retrieval using personal identifiers. All audit logs are stored on the FAA cloud. UAFR-Utility users cannot retrieve case file records using personal identifiers when querying the UAFR-Utility. Audit logs can only be queried in the UAFR-Utility using the UAFR Tracking ID or Site ID.

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[8], 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[9].

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 UAFR-Utility is a privacy-sensitive system because it collects, uses, disseminates, and retains PII from *UAFR Authorized Users*, *UAFR Public Members*, and *UAFR UAS Operators* to designate UAFRs for eligible fixed site facilities. Policies, procedures and practices for information storage, data use, access, notification, retention and disposal are described in this PIA.

The FAA protects records subjects' Privacy Act rights in accordance with the following System of Records Notice (SORN):

DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002 covers user account records about Members of the Public that choose to create UAFR-Utility accounts to participate in the UAFR designation process. The records may include the following PII about *UAFR Authorized Users*, *UAFR Public Members*, and *UAFR UAS Operators*: names, email addresses, and passwords.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the UAFR-Utility. Additionally, basic personal identifiers (names and email addresses) collected to create user accounts and submit public comments on Conditionally Approved UAFRs are covered by a separate PIA that is currently undergoing DOT adjudication related to the NPRM corresponding to the UAFR-Utility, titled

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

Applications for Designation – Prohibit or Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed-site Facility Notice of Proposed Rulemaking.

A Privacy Act Statement is posted on the UAFR-Utility website stating the authority to collect information during user registration under the Privacy Act of 1974.

All designated UAFRs are published in the Federal Register and FAA Order Joint Order (JO) 7400.12,[10] *Unmanned Aircraft Flight Restriction Designations*, including status as approved, expired, or cancelled, a summary of all associated public comments and responses, as well as a reference to the UAFR-U via a website link. However, no personal identifiers are published – only information about the fixed site facility and the UAFR activation.

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 UAFR-Utility is a cloud-based, web portal that collects PII directly from individual users (e.g., Members of the Public with user accounts) and allows individuals access to their own data, enabling and requiring them to correct, amend, or delete that data, as appropriate. Individuals can contact an associated FAA help desk for issues experienced during individual participation or if redress is required, as well as a Frequently Asked Questions (FAQ) web page that offers instructions.

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

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

FAA 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

[10] Once part 74 has been finalized, an electronic version of JO 7400.12 will be available on FAA's website at https://www.faa.gov/air_traffic/publications/.

- 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 has authorized the FAA Administrator to develop systems and/or tools to support the designation of UAFRs for eligible fixed site facilities. The UAFR-Utility addresses the unique demands of the FAA's workforce and operates under the authority of 49 United States Code (U.S.C.) 44802, Section 2209, p. 1203.

The UAFR-Utility is an interactive, end-to-end solution for the management of Unmanned Aircraft Flight Restrictions (UAFRs), in accordance with procedures stated in the regulatory text of Title 14 of the Code of Federal Regulations (14 CFR) Part 74, *Designation of Unmanned Aircraft Flight Restrictions.* The UAFR-Utility fulfills Part 74 requirements by providing a cloud-based web portal to designate UAFRs for eligible fixed site facilities.

The UAFR-U system collects basic personal identifiers from members of the public, including *UAFR Authorized Users*, *UAFR UAS Operators*, and *UAFR Public Members*. PII records collected from *UAFR Authorized Users* include name and contact information and can be collected from the following transactions: Eligibility Determination (1) and Amendment (6). PII records collected from *UAFR UAS Operators* include name and contact information and can be collected from the following transactions: Access (9). PII records collected from *UAFR Public Members* include name and contact information and can be collected from the following transactions: Public Notice and Comment (2). The UAFR-Utility maintains names and email addresses of federal employees and contractors for UAFR-Utility system access. FAA credentials are exchanged with FAA MyAccess.

The FAA uses this access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the UAFR-Utility and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

The PII in the UAFR-Utility is not used for 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 collects the minimum amount of information from individuals to support the FAA's designation of UAFRs for eligible fixed site facilities. The UAFR-Utility only uses and retains basic personal identifiers to create user accounts, and to assign points of contact for the fixed site facilities requesting UAFRs. All PII collected is required, not optional or voluntary. The FAA maintains different types of records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules[11] (GRS):

The following disposition schedules are governed by NARA GRS 3.1, *General Technology Management Records*, November 2019. The FAA retains UAFR-U information technology development project records temporarily according to disposition schedule, DAA-GRS-2013-0005-0007. These records are disposed of 5 years after the system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes. However, this information may be retained for a longer period if retention is required for business use.

The FAA retains UAFR-U information technology operations and maintenance records temporarily according to disposition schedule, DAA-GRS-2013-0005-0004, approved November 2019. These records are disposed of 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded. However, this information may be retained for a longer period if retention is required for business use.

The FAA retains UAFR-U configuration and change management records according to disposition schedule, DAA-GRS-2013-0005-0005, approved November 2019. These records are disposed of 5 years after the system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes. Longer retention is authorized if required for business use.

The FAA retains UAFR-U data administration records (i.e., all documentation for temporary electronic records and documentation not necessary for preservation of permanent records) temporarily according to disposition schedule, DAA-GRS-2013-0005-0003, approved November 2019. These records are disposed of 5 years after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. Longer retention is authorized if required for business use.

The following disposition schedules are governed by NARA GRS 3.1, *Information Systems Security Records*, November 2019. The FAA retains UAFR-U systems and data security records are maintained temporarily according to disposition schedule, DAA-GRS-2013-0006-0001. These records are disposed of 1 year after the system is superseded by a new

[11] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and in order to promote consistent retention practices.

iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

The FAA retains UAFR-U computer security incident handling, reporting and follow-up records are maintained temporarily according to disposition schedule, DAA-GRS-2013-0006-0002. These records are disposed of 3 years after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use. The FAA retains UAFR-U system access records (systems not requiring special accountability for access) are maintained temporarily according to disposition schedule, DAA-GRS-2013-0006-0003. These records are disposed of when the business use case ceases. The FAA retains UAFR-U incremental backup files (e.g., system backups and tape library records) are maintained temporarily according to disposition schedule, DAA-GRS-2013-0006-0005. These records are disposed of them when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

The FAA retains UAFR-U Full backup files (e.g., system backups and tape library records) are maintained temporarily according to disposition schedule, DAA-GRS-2013-0006-0006. These records are disposed of when a second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

The following disposition schedules are governed by NARA GRS 5.7, *Administrative Management and Oversight Records*, approved March 2022. The FAA retains UAFR-U Federal Register notices other than proposed and final rules are maintained temporarily according to disposition schedule, DAA-GRS- 2017-0012-0004, approved March 2022. These records are disposed of when they are 1 year old, but longer retention is authorized if required for business use.

UAFR Unauthorized Access Reports and Annual Reports will be covered by an agency-wide schedule for FAA geospatial records. The record schedule is currently being drafted with plans to submit to NARA. These records will be treated as permanent until the draft schedule is approved by 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 PII in the UAFR-Utility is used to support the designation of UAFRs for eligible fixed site facilities, requiring participation in the designation process by *UAFR Authorized Users*, and including participation of *UAFR Public Members*, and *UAFR UAS Operators*. The FAA does not use the PII for any other purpose.

Access and authentication PII collected by the FAA is used as specified by the DOT's system of records notice, DOT/ALL 13, Internet/Intranet Activity and Access Records.

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 this 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 approved investigations 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 negation 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; and

• To other government agencies where required by law.

Lastly, the Department has published 15 routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at Privacy Act System of Records Notices | US Department of Transportation.

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 applies and maintains several controls with the UAFR-Utility to ensure accurate, relevant, timely data of high quality. Data integrity and information security are preserved to ensure no changes to data without authorization. All data fields within the UAFR-Utility are programmed with rules to ensure proper data collection (e.g., use of drop-down menu selections rather than free text wherever feasible, disclaimers about the input of personal identifiers in free text fields). The FAA uses a quality assurance/quality control (QA/QC) process to verify data accuracy and update as necessary. PII is collected directly from individual users (e.g., Members of the Public with user accounts).

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 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 UAFR-Utility 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 the UAFR-Utility. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures and posture of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues the UAFR-Utility 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 UAFR-Utility 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 UAFR-Utility as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Andrew Shutt
System Owner, Program manager, Air Traffic Organization
andrew.c.shutt@faa.gov
(817) 913-9636

Prepared by: Essie Bell, Acting FAA Chief Privacy Officer

Approval and Signature

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

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.05.06 15:49:45 -04'00'