U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Central Altitude Reservation Function (CARF)

Responsible Official

Melissa Matthews
System Owner
Email: melissa.matthews@faa.gov
Phone Number: 202-267-0764

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Air Traffic Control (ATO) Central Altitude Reservation Function (CARF) system operates under authority 49 U.S. Code § 40101. It is a system for coordination of Altitude Reservation (ALTRV) requests and special military operations, both nationally and internationally. The FAA CARF Office is responsible for coordinating military and civilian ALTRVs for operations that depart their area of jurisdiction and for ALTRVs that operate within US-controlled airspace. Altitude reservations are used for mass movement of aircraft or special requirements, which cannot be met satisfactorily without an altitude reservation. The majority of ALTRVs are requested by the Department of Defense (DoD).

The FAA is publishing this Privacy Impact Assessment (PIA) for CARF in accordance with Section 208 of the E-Government Act of 2002 because the system collects Personally Identifiable Information (PII) from members of the public, specifically representatives of private companies requesting Altitude Reservations.

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 PII. The goals accomplished in completing a PIA include:

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

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

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

Introduction & System Overview

The CARF Program was established in the 1960s and is the single point of contact for coordination of ALTRV requests and special military operations. The CARF Office is responsible for coordinating military and civilian ALTRVs for operations that depart their area of jurisdiction and for ALTRVs that operate within United States-controlled airspace. Altitude reservations are used for mass movement of aircraft or special requirements, which cannot be met satisfactorily without an altitude reservation. The vast majority of ALTRVs are requested by the DoD. In these cases, the DoD requests may come via phone or email to a CARF Specialist. Other federal government agencies can request an ALTRV in cases of emergency[2]. The FAA can also process an ALTRV request for commercial companies, such as SpaceX. However, in this case, the commercial company must submit its ALTRV request through its DoD liaison, who is a DoD employee. The DoD liaison would then submit this request to the CARF specialist to process, because private companies cannot submit a request directly to CARF.

CARF serves as a centralized, one-stop system for submitting, processing, and managing all ALTRV requests. The system supports CARF Specialists in their primary mission of separating and de-conflicting military and civilian flight operations that require altitude blocks, ensuring that all missions are safely coordinated. The expanding operational role of CARF—driven by an increase in military and commercial ALTRV requests—requires greater automation and processing efficiency to preserve the safety and capacity of the National Airspace (NAS).

CARF is used to:

[2] Per FAA Order 7610.4, Section 3−7−3. EMERGENCY ALTITUDE RESERVATIONS- *CARF or an ARTCC/CERAP/HCF may approve a request for an emergency ALTRV if the safety of life or property is threatened. Operations, such as search and rescue, hurricane evacuation, or mass air evacuation, may be considered in this category.* ARTCC- Air Route Traffic Control Center; CERAP – Combined Center/Radar Approach Control; HCF – Honolulu Control Facility.

- Receive and store ALTRV requests;
- Perform automated and manual de-confliction of airspace;
- Coordinate between FAA facilities, DoD mission planners, and commercial entities;
- Issue approvals or coordinate final decisions based on FAA Order 7610.4, *Special Operations Handbook*, and relevant Letters of Agreement (LOAs) and Memoranda of Understanding (MOUs); and
- Generate and transmit Notices to Air Missions (NOTAMs) when required.

CARF collects PII from:

- Members of the public (e.g., representatives of private companies requesting ALTRVs);
- FAA and federal government employees submitting or processing ALTRV requests; and
- FAA employees and contractors for system login and access control.

PII collected includes:

- Full name of the ALTRV requestor;
- Business email address;
- Work telephone number;
- Aircraft call sign (contained in the flight plan); and
- Planning Officer's name and contact number (included in remarks).

Typical Transaction

A typical transaction begins when a CARF Specialist receives an ALTRV request via email to the CARF functional mailbox, 7-awa-carf@faa.gov; the email includes the Requestor's Name and Contact Information (email address and phone number). The ALTRV request also includes the following data elements: aircraft call sign, number and type of aircraft, departure point, route of flight, destination, departure time, and remarks. The "Remarks" section includes the FAA Planning Officer's name and work telephone number. The PII collected includes the full name of the ALTRV requestor, business email address, phone number, aircraft call sign (contained in the flight plan), and the Planning Officer's name and contact number. The request is manually entered into the CARF database, so it can be simultaneously accessed from different CARF client workstations.

Once the ALTRV is entered into the CARF system, the system performs a process called "de-conflicting," which means the CARF system checks the proposed mission altitude and flight path against all other missions scheduled for the same day; the CARF system then alerts the CARF Specialist of conflicting mission segments. Although the system will

automatically indicate if there are any conflicts, the CARF Specialist also performs a manual review. If there is a conflict or a question about the ALTRV request, the FAA CARF Specialist contacts the ALTRV requestor by phone or email, depending upon the priority of the ALTRV request. The CARF Specialist notifies any FAA facilities that would be affected and obtains their concurrence for the ALTRV request. The CARF Specialist also assesses if CARF has the final approval authority for the ALTRV request. FAA Order 7610.4, "Special Operations Handbook" provides specific guidance for ALTRV issuance and approvals.

Once an ALTRV request is approved, the CARF Specialist determines if a Notice to Air Mission (NOTAM) is required. The NOTAM describes the ALTRV at least three days in advance of the approved ALTRV date. The NOTAM is then sent to the Aeronautical Information System Replacement (AISR) to broadcast the NOTAM via an FAA Service B message. The CARF Specialist also notifies the Requestor. The CARF NOTAMs are available to members of the public at FAA NOTAM search on the CARF NOTAM link: Federal Aviation Administration: NOTAM Search.

CARF records are ALTRV requests for altitude adjustment, are not records about individuals and are compared by the date of the request to ensure there are not multiple ALTRV requests for the same day.

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, 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.

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 PI). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

CARF is not a publicly accessible system. In addition, PII collected from members of the public, FAA personnel, and federal government requestors is not retrieved by a unique identifier. Access to the CARF system is restricted to authorized users, and a Privacy Act Statement is provided at the point of ALTRV login.

The CARF system automatically runs a "de-confliction" process, analyzing the requested flight path and altitude against other scheduled operations for the same timeframe. Any conflicts are flagged by the system and then manually reviewed by the CARF Specialist. If clarification or adjustments are needed, the Specialist contacts the requestor via phone or email, depending on the urgency of the mission.

The FAA also promotes transparency through the publication of appropriate privacy compliance documentation. This PIA is published in accordance with the E-Government Act of 2002, to ensure public awareness of the information handling practices associated with the CARF system, while the Department of Transportation (DOT) has published the System of Records Notice (SORN) *DOT/ALL 13, Internet/Intranet Activity and Access Records* (67 FR 30757, May 7, 2002), which applies to information collected and maintained in support of FAA systems, and it covers system access records maintained in CARF.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The FAA collects limited PII directly from members of the public, FAA employees, and federal personnel as part of the ALTRV coordination process via CARF. CARF is primarily focused on mission-specific flight information. PII such as name, email address, and phone number of ALTRV requestors may be included in submitted documents and stored within the system.

The only records within CARF that are retrieved by unique identifier are those collected for access and authentication, which are covered under System of Records Notice (SORN) DOT/ALL 13, Internet/Intranet Activity and Access Records (67 FR 30757, May 7, 2002)

Under the Privacy Act of 1974, individuals may request access to their records as it pertains to system access by submitting a written inquiry to:

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

The request must include:

- Full name
- Mailing address
- Phone number and/or email address
- A detailed description of the records sought, and if possible, the location or context of the records

Contesting Record Procedures

Individuals who believe information relating to system access in CARF is inaccurate or incomplete may request corrections. These requests should be submitted in writing with an explanation of the correction sought to:

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

All requests will be processed in accordance with the Privacy Act and applicable FAA and DOT privacy policies.

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.

The CARF is authorized under Title 49 United States Code (U.S.C.) § 40101, which outlines the FAA's authority to regulate and manage the safe and efficient use of the NAS. The primary purpose of CARF is to provide automated and manual coordination, de-confliction, and approval of ALTRVs for military, government, and commercial users requiring special airspace accommodations.

To do so, CARF collects only the PII necessary (full name of requestor, email address, phone number) to receive and store ALTRV requests, perform automated and manual de-confliction of airspace and coordinate between FAA facilities.

CARF supports the FAA's air traffic and national defense responsibilities by managing special operations flight requests across NAS sectors. To accomplish this mission, CARF processes and collects PII associated with requestors and FAA personnel who access or interact with the system.

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

CARF is designed to collect the minimum amount of PII necessary to fulfill its mission of processing and coordinating ALTRV requests. The system limits data collection to operational details such as names, contact information, and flight mission data required to manage airspace safety and scheduling.

CARF maintains records under approved NARA schedules. For non-regulatory NOTAMs, these records capture regular notices of changes in the National Airspace System, including domestic, military, and international updates. Once a NOTAM is canceled or expires, the records are designated as temporary and must be destroyed no sooner than five years after the cutoff date; altogether longer retention is permitted if necessary.

Additionally, the system follows General Records Schedule (GRS) 3.2, Information Systems Security Records Item 30: System Access Records are included. These are also classified as temporary and are destroyed once business use ceases, ensuring that system access data is retained only for as long as operationally required.

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.

Primary records in CARF are not covered by the Privacy Act. FAA collects PII from individuals, as noted in the "Purpose Specification" section above, and FAA does not use this information for any other purpose. Access to the CARF system is restricted to authorized users. 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, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignments 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.

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).

To maintain the accuracy of ALTRV data, CARF Specialists perform a combination of automated and manual reviews to identify routing conflicts and validate request details. If clarification or adjustments are needed, the Specialist contacts the requestor via phone or email, depending on the urgency of the mission. These reviews ensure the coordination of safe flight operations across the NAS.

Information entered in CARF system includes contact names, aircraft call signs, mission parameters, and coordination details that are actively verified throughout the deconfliction and approval process. Persons who wish to correct this information may do so via email to the CARF functional mailbox, 7-awa-carf@faa.gov.

Administrative records and audit logs are maintained according to approved NARA schedules. Role-based access and system audit trails help safeguard data integrity by limiting data modifications to authorized FAA personnel and contractors.

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 does not allow access through either the Internet or Intranet to the information stored in the CARF system. In addition to physical and logical access controls, CARF limits access to PII according to job function.

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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 23, 2020 (includes updates as of December 10, 2020).

Access to the CARF application is limited to those with appropriate security credentials, an authorized purpose, and a need to know. The FAA deploys role-based access controls in addition to other protection measures reviewed and certified by the FAA's cybersecurity professionals to maintain the confidentiality, integrity, and availability requirements of the system. The web application function is only accessible to FAA-authorized personnel.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for the governance and administration of FAA Order 1370.121B, FAA Information Security and Privacy Program and Policy which provides implementation guidance for the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the FISMA, Office of Management and Budget (OMB) mandates, NIST and other applicable DOT and FAA information and information technology management procedures. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, and processing privacy data.

Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of Privacy ICAO Address Program in accordance with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Melissa Matthews
Manager, Aeronautical Products, AJM-336
FOB-10B, 4W21HN
2022670764 (O) 2028532441 (C)

Prepared by: Michael Bjorkman, Acting Chief 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: 2025.10.06 12:37:24 -04'00'