U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

FAA

FALCON

Responsible Official

Kimberly K. Walton-Emminger
Email: kimberly.k.walton-emminger@faa.gov
Phone Number: (858) 381-2404

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 Organization (ATO), owns the Falcon mission support system installed and used at FAA air traffic control facilities throughout the National Airspace System (NAS). The system enables the replay of NAS radar data synchronized with voice recordings of conversations between Air Traffic Controllers and pilots. The recorded audio conversations consist of voice navigational instructions from Air Traffic Controllers and responses from the flight crew (such as a pilot). These recordings could additionally contain Personally Identifiable Information (PII) provided by the pilot such as full name, flight location (e.g., origin, destination, path) and aircraft tail (or registration) number. The replays are used for air traffic quality assurance (ATQA), safety analysis, controller training, and investigation of safety events.

The FAA developed this Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 because Falcon collects PII from members of the public, most notably pilots (civilian and military) of flights throughout the NAS.

What is a Privacy Impact Assessment?

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

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

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

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

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

Introduction & System Overview

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 uses Falcon to meet its mission regarding air traffic safety. Falcon is a safety support system for monitoring operational radar positions through available playback information synchronized with audio files.

These audio exchange replays between Air Traffic Controllers and pilots PII from the pilots. This information could include the pilot's full name, aircraft tail (or registration) number, the flight's location (e.g., origin, destination, path), among other identifiable details.

Falcon is hosted by the Operational Analysis and Reporting System (OARS) on the FAA Cloud Services (FCS) in the Amazon Web Services (AWS) Government Community Cloud (GCC) – West. The system is managed by FAA's Safety Support Tools (AJI-3340) and supported by an FAA contractor under Safety Services Support.

User Access

Falcon is used by the FAA federal and contractor workforce on the agency's internal network and is not accessible from the Internet or to the public. FAA employees and contractors access the Falcon web application through the Operational Analysis and Reporting System (OARS) Portal which leverages FAA MyAccess/Okta for Multifactor Authentication (MFA) and Single Sign-On (SSO) in compliance with Executive Order 14028. Falcon user access permissions are managed through the Comprehensive Electronic Data Analysis and Reporting (CEDAR) system.

A PII Data Sharing Agreement exists between OARS and Falcon to facilitate the sharing of user authentication information. The PII data elements shared from OARS to Falcon include individual email address (i.e., first name, last name, middle initial as applicable) and FAA MyAccess/Okta MFA authentication token information transmitted via hypertext transfer protocol secure (HTTPS).

Typical Transaction

Falcon replays allow FAA users to view air traffic radar—similar to what an Air Traffic Controller sees on the radar scope—and to listen to the pilot-controller audio exchange. A user performs the following steps to create a replay:

- The user specifies the facility, radar sensor, start date and time, and replay length in minutes.
- The user bookmarks the replay by giving it a name and adding a description and one or more keyword tags.
- The user then locates and adds the corresponding audio for the specified facility and radar sensor. Audio is not a required parameter.

Quality Assurance (QA) analysts use Falcon replays to review and analyze air traffic events reported in Preliminary ARIA Reports (PAR) and Mandatory Occurrence Reports (MOR) in CEDAR. Replays are also used for controller safety training and for the development, evaluation, and improvement of Air Traffic Control (ATC) procedures.

A Summary of Other Transactions

Falcon includes a recording feature that exports a compressible MP4 file specifically used by executive leadership to review. This feature is limited to investigators and QA teams. To improve training efficiency, a bookmark link to the application may be added within training records.

Falcon has two subsystems: Search and Rescue (SAR), which enables Falcon to accurately depict the position of aircraft during a selected time period, and Aviation Risk Identification and Assessment (ARIA), which calculates the probability of risk of collision.

Replay data is available for 45 days before automatic deletion. Details of saved bookmarks are held in the Falcon database. User login information is encrypted and is not accessible outside the Falcon system.

Falcon manages user access through CEDAR and tracks activities of each user. User passwords are encrypted via FAA Directory Services Active Directory and user information is not accessible outside of Falcon. Access records for FAA employees and contractors are retained as temporary records and destroyed when business use ceases.

Sensitive Flight Data

Falcon processes certain data elements that are classified as Sensitive Flight Data (SFD) under FAA policy. The following data elements collected or displayed through Falcon are considered SFD:

- **Aircraft Call Sign:** The unique identifier broadcast by an aircraft during radio communications with Air Traffic Control.

- **Aircraft ID/Tail Number:** The registration number assigned to an aircraft which can be used to identify the aircraft's owner.
- **Route of Flight:** Information about an aircraft's origin, destination, and flight path.

Falcon handles SFD in accordance with FAA policy and Enterprise Information Management (EIM) data governance requirements.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3,[2] sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.[3]

Transparency

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

The FAA takes steps to ensure the transparency of Falcon to the aviation community and the public. Falcon replays include audio exchanges from the Digital Audio Legal Recorder Remote Audio Access System (DRAAS) and National Voice Recorder (NVR) which contain pilot-controller voice recordings. In the unlikely event a member of the public, typically a solicitor or someone dialing a wrong number, calls an air traffic facility on an internal FAA line that is not accessed by the public, the contacted FAA employee informs them they have contacted an air traffic facility, and the conversation is being recorded.

In addition, the FAA published this PIA to demonstrate its commitment to providing appropriate transparency about its use of Falcon and the personal information contained in the system. These recordings are not retrieved by identifiers, so no System of Record Notice

[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

(SORN) coverage is required on the operational side. Lastly, the records pertaining to access are managed in accordance with the Department of Transportation's (DOT) System of Records Notice (SORN) DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002).

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.

Through the replay function of Falcon, the FAA collects information from pilots who interact with ATC personnel. The voice recordings capture any information provided by the pilots or the ATC personnel. Pilots may provide call signs and tail number identifiers to ATCs. This information could be considered PII, as it may be linkable to individuals via other data sources; however, this information is not retrievable via a personal identifier within Falcon and is not linked to any outside data source that could result in the identification of an individual. In addition, FAA ATCs may provide their two-letter operating initials (a unique identifier) to the pilots.

The Falcon system manages user access through CEDAR and tracks activities of each user in an internal database. The FAA collects information to create user accounts directly from those employees and contractors, including name (first and last), username, and password.

As noted above, records pertaining to FAA employees/contractors Falcon access are managed in accordance with the Department of Transportation's (DOT) System of Records Notice (SORN) DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002).

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

Notification Procedure (for access to records):

Federal Aviation Administration
Privacy Office
800 Independence Avenue, 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 (for redress/amendment of records):

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

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

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 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 recordings are a record used for air traffic quality assurance (ATQA), training, and safety investigations.

The FAA uses the Falcon system and the information used and stored therein pursuant to the following legal authorities:

1) Title 49 United States Code (U.S.C.) § 40101, Policy, which covers matters relating to aviation safety;
2) Title 49 U.S.C., Transportation, Subtitle VII — Aviation Programs, Part A — Air Commerce and Safety, § 40113, which covers administrative activities with respect to security duties and powers designated to be carried out by the Administrator of the Federal Aviation Administration;
3) Title 49 U.S.C. § 44506, Air Traffic Controllers, which covers qualifications, selection and appointment, training, certification and licensing, duties and responsibilities, and medical standards of air traffic controllers; and
4) Title 5 (Government Organization and Employees), U.S.C.; Title 32 of the Code of Federal Regulations (National Defense); and Title 40 U.S.C. 486c (Policies, regulations and delegations), which authorizes the collection of user authentication information for system access.

The FAA is responsible for maintaining records of Falcon system users and audit information for the purposes described in DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002). These records may include username, user ID, employee ID, and email address.

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.

DOT/FAA requests the minimum amount of information necessary to meet its legal obligations and business requirements. Falcon recordings capture call-sign and tail-number information from pilots, as well as the unique two-letter operating initials provided by FAA ATCs. While Falcon may capture any information spoken by pilots or FAA ATCs, none of the information provided is retrievable by identifiers within Falcon. For user authentication, Falcon receives individual email addresses (i.e., first name, last name, middle initial as applicable) from the OARS Portal via FAA MyAccess/Okta.

The FAA has an approved records retention and disposition schedule with the National Archives and Records Administration (NARA). Falcon follows these retention schedules:

- **Audit Logs:** General Records Schedule (GRS) 3.1, General Technology Management Records (DAA-GRS-2013-0005-0004), item 20 – Information technology operations and maintenance records. These records are temporary and are destroyed 3 years after agreement, control, measures, procedures, project, activity or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.
- **System Access Records:** GRS 3.2, Information Systems Security Records (DAA-GRS-2013-0006-0003), item 30 – System Access Records. These records are temporary and are destroyed when business use ceases.
- **Replay Data:** Available for 45 days before automatic deletion.
- **Reports:** GRS 5.2, Transitory and Intermediary Records (DAA-GRS-2022-0009-0002), item 020 – Intermediary Records. These records are temporary and are destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later.

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 recordings are used for air traffic quality assurance, training and safety investigations. Falcon does not allow information to be added, deleted, or revised by its general users. Any PII collected in these recordings are part of the exchange between pilots and ATCs and nothing additional can be attached to/included in it.

The sharing of FAA employee and contractor user account and access information within the system is in accordance with Department of Transportation SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002). 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 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.

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).

Falcon captures voice recordings of interactions between pilots and FAA ATCs. The information provided by pilots, such as call-signs and tail-numbers, or that which is provided by FAA ATCs, such as the two-letter operating initials that uniquely identify each ATC, are presumed accurate. Either party may ask for clarification of the information provided, as needed, to ensure accuracy. The information captured within the recordings cannot be changed. Each recording is time-stamped with the date and time that the call took place.

There is no manual data entry in the Falcon system.

Falcon manages user access through CEDAR and tracks the activities of each user. The collection and retention of PII in Falcon is limited to the minimum use necessary to

accomplish its purposes. Only personnel whose job duties require the use of PII are assigned the privileges necessary to access relevant PII.

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 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 Information Systems and Organizations, dated September 2020.

Falcon is used by the FAA federal and contractor workforce on the agency's internal network and is not accessible from the Internet or to the public. System users access the Falcon web application through the OARS Portal which leverages FAA MyAccess/Okta for MFA and SSO.

The recording feature is limited to AJI-1 investigators and QA teams.

Falcon is categorized as a Moderate-risk system for Confidentiality, Integrity, and Availability. The system was granted an Authority to Operate (ATO) on May 19, 2023, with an expiration date of May 19, 2026. Falcon was granted its ATO after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A) process. FAA Security Personnel audit the Falcon 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 107-347), 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 are consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance about their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. FAA will conduct periodic privacy compliance reviews of Falcon with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Kimberly K. Walton-Emminger
System Owner
Falcon
Safety Support Tools Program Office, AJI-3340

Prepared by: Kimberly K. Walton-Emminger (System Owner)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.05.04 15:08:06 -04'00'