U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Air Traffic Organization (ATO)/Enterprise Services (AJM-3/AJM-311)

Voice Recorder Replacement Program/Digital Audio Legal Recorder (VRRP/DALR)

Responsible Official

Wayne Findley
Email: wayne.findley@faa.gov
Phone Number: (405) 954-9481

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 Voice Recorder Replacement Program/Digital Audio Legal Recorder (VRRP/DALR) voice recording system installed and used at FAA air traffic control facilities throughout the National Airspace System (NAS). The system records audio conversations consisting of voice navigational instructions from Air Traffic Controllers and responses from the flight crew (such as a pilot) confirming that they received the instruction. The conversations ensure planes are properly spaced, where they are to take off or land and altitude at which they should be flying and help determine whether instructions were timely, appropriate, confirmed, and followed. The recordings are used for air traffic quality assurance (ATQA), legal compliance, search/rescue, and public requests made under the Freedom of Information Act (FOIA).

The FAA is developing this Privacy Impact Assessment in accordance with Section 208 of the E-Government Act of 2002 because VRRP/DALR collects information that may be considered Personally Identifiable Information (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

[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

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.

The FAA uses VRRP/DALR to meet its mission regarding air traffic control. VRRP/DALR is a commercial off-the-shelf solution meeting the FAA requirements for digital audio recording for legal/compliance purposes for calls to air traffic control (ATC) facilities. The system uses hardware platforms and software applications consisting of one or more recorders, an applications server module, and one or more client workstations to securely record, store, retrieve, playback, duplicate, erase, and manage operational and administrative voice data.

The VRRP/DALR follows guidance provided by FAA through various FAA Orders and manuals pertaining to flight information.

System Access by FAA Employees/Contractors

VRRP/DALR is not accessible from the Internet or to the public; it is only accessible to the FAA federal workforce and contract workforce on the FAA's internal network. FAA employees and contractors access the system with a username and password. In addition, the system assigns a user ID and PrivilegeProfileID to each user; this information is not accessible to the user.

Typical Transaction

From a system workstation, users login to the system graphical user interface (GUI) application known as NICE Inform. NICE Inform contains several modules: Monitor, Reconstruction, Organizer, Audit, System Administration, and User Administration. Access to the modules and access rights within the modules are restricted on an individual user basis. Users of the system include Air Traffic Quality Assurance, Air Traffic Management, and Air Traffic System Specialists, who maintain the system.

The main use of the recorder is to retrieve audio for review, training, and/or analysis. The recorded audio conversations consist of voice navigational instructions from Air Traffic and responses from the flight that received the instruction. The pilots identify themselves by flight number, while FAA Air Traffic Controllers identify themselves by their two-letter operating initials; however, if they choose to provide any additional information, it would also be recorded. Spoken instructions between the ATCs and pilots reference the altitude, direction, runway, or taxiway of a particular aircraft.

An FAA supervisor may also access near-real time playback and may listen in on a conversation for awareness and assistance to the Air Traffic Controller.

A Summary of Other Transactions

From the Organizer module, a user with appropriate access rights can replay the audio segments and/or create Waveform Audio File (WAV) file(s) of the audio. During the WAV file creation process, the user can choose to add audio statements to the file. This is typically done when creating a legal recording per FAA Order JO 8020.16 (as amended). The incident folders remain on the system until manually deleted.

Using the Monitor module, a user, depending on the user rights, can listen to audio from any recorded position in near real-time. This is typically done by a supervisor for listening to an ongoing issue with an aircraft or to provide feedback to a controller for training purposes.

Details of saved incidents[2] are held in the Inform Incident database. This database is part of the VRRP/DALR system but is not accessed directly. User login information is encrypted,

[2] An incident is considered anything an investigator might be tasked to investigate, such as a pilot deviation, loss of separation, aircraft accident, etc.

and the information is not accessible outside the VRRP/DALR system. This database contains the following data elements: Creator User ID, Creation Date, Creator First Name, Creator Last Name. The Incident database contains details of an incident. These details do not include PII but may include location, latitude, and longitude of the incident for playback purposes. The actual call recordings are not stored in the database.

Audio is available in the Reconstruction module for 45 days before automatic deletion. When the user requires audio for additional time, such as when the recording is tied to an investigation of an incident, they copy the audio to Organizer module folders called "incidents" in the application. Audio retrieved for investigations is copied to removable media and archived. The original copy of the audio on the DALR system is manually deleted according to established retention schedules.

Lastly, VRRP/DALR manages user access and tracks activities of each user in an internal database. User passwords are encrypted, and the user information is not accessible outside the VRRP/DALR system. Tracked user details contain the user ID and username (first and last). Access records for FAA employees and contractors are retained as temporary records and destroyed when the business uses ceases.

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[3], 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[4].

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.

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

The FAA takes steps to ensure the transparency of VRRP/DALR to the aviation community and the public. For its public access telephone line, FAA provides notice that calls received on that line are recorded and the caller provides consent by continuing with the call. In the unlikely event a member of the public, typically a solicitor or wrong number, calls an air traffic facility on an internal FAA line that is not public access, the contacted FAA employee informs them they have contacted an air traffic facility and the conversation is being recorded.

In addition, the FAA has published this PIA to demonstrate its commitment to provide appropriate transparency about its use of VRRP/DALR. Lastly, the records pertaining to VRRP/DALR 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 30757 (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 call recording function of VRRP/DALR, 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 is may be linkable to individuals via other data sources, however this information is not retrievable via a personal identifier within VRRP/DALR 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 VRRP/DALR manages user access and tracks activities of each user in an internal database. FAA collects information to create user accounts directly from those employees and contractors, including name (first and last), username, and password. In addition, the VRRP/DALR system assigns certain identifiers to users, such as user ID and PrivilegeProfileID. The system-generated identifiers are not accessible by the user.

As noted above, records pertaining to FAA employees/contractors VRRP/DALR 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 30757 (May 7, 2002). 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 VRRP/DALR 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

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 public record used for air traffic quality assurance (ATQA), search/rescue, legal compliance, and public requests under the Freedom of Information Act (FOIA).

The recorded audio conversations consist of voice navigational instructions from Air Traffic and responses from the flight that they received the instruction. The conversations ensure planes are properly spaced, where they are to take off or land and altitude at which they should be flying. The recorder tracks which audio source was recorded and what time the conversation took place. As for PII or potential PII captured in the call recordings, the pilots provide flight number or call sign information, while the FAA ATC Specialists provide their two-letter operating initials, which serve as a unique identifier. None of this information is retrievable in VRRP/DALR.

The FAA is responsible for maintaining records of VRRP/DALR system users and audit information for the purposes described in DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002). These records may include username, user ID and Privilege Profile ID.

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. VRRP/DALR recordings capture call-sign and tail-number information from pilots, as well as the unique two-letter operating initials provided by FAA ATCs. While VRRP/DALR may capture any information spoken by pilots or FAA ATCs, none of the information provided is retrievable within VRRP/DALR. For example, VRRP/DALR cannot retrieve call-sign information captured within the recordings.

The FAA has an approved records retention and disposition schedule with the National Archives and Records Administration (NARA). VRRP/DALR digital voice recordings are destroyed when 45 days old, while VRRP/DALR analog recordings are destroyed when 15 days old under FAA record schedule N1-237-02-5.

VRRP/DALR access records for FAA employees and contractors are retained as temporary records and destroyed when the business uses ceases as specified under NARA's General Record Schedule 3.2, *Information Systems Security Records, Item 30: System Access Records*, under disposition authority DAA-GRS-2013-0006-0003.

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.

As noted in the Purpose Specification section above, the recordings are a public record used for air traffic quality assurance, search/rescue, legal compliance, and public requests under the Freedom of Information Act (FOIA). VRRP/DALR call recordings are not used for any other purpose.

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(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.

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).

VRRP/DALR 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 a 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.

DALR manages user access and tracks activities of each user in an internal database. The user information is not accessible outside the VRRP/DALR system.

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 VRRP/DALR system has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. VRRP/DALR was granted its ATO after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). FAA Security Personnel audit the VRRP/DALR system to ensure FISM 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. FAA will conduct periodic privacy compliance reviews of VRRP-DALR with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Wayne Findley
System Owner
Manager, NAS Communications Team, AJW-1530

Prepared by: Barbara Stance, FAA 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: 2024.04.17 15:19:08 -04'00'