# U.S. Department of Transportation

# Privacy Impact Assessment

## Federal Aviation Administration (FAA)/ Air Traffic Organization (ATO)

## Operational and Supportability Implementation System (OASIS II)


### Responsible Official

Stephen C. Ryan
Acting Manager
Flight Services In-Service Management, AJR-B2
202 267-6474

### Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov


CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2019.06.20 13:11:35 -04'00'

## Executive Summary

The Federal Aviation Act of 1958 gives the Federal Aviation Administration (FAA) the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. One of the programs that helps the FAA fulfill these responsibilities is the Operational and Supportability Implementation System (OASIS II). OASIS II is a system in the National Airspace System (NAS) which processes and displays weather products, tracks flight service functional daily activities and time on position, provides flight planning (departure, destination, route information), regulatory information (flight path restrictions, air traffic control system status, airport status information and operational Notices to Airmen), and OASIS equipment status information. OASIS II consists of storage and processing equipment in the Anchorage Air Route Traffic Control Center (ZAN) and workstations at the 17 Flight Service Stations (FSS) located throughout Alaska. OASIS II is used strictly by FAA Flight Service Specialists in Alaska to provide weather briefing and flight planning services to general aviation pilots. Flight Plans are required for every flight that uses Instrument Flight Rules (IFR) procedures and is strongly recommended for all other flights. Flight plans contain personally identifiable information (PII) that is collected and maintained for emergency response purposes by FAA regulations. Use of the PII in OASIS II is limited to emergencies such as a search-and-rescue, incident, and/or accident investigations.

## 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:*

- *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*

[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).

- *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

**Overview of OASIS**

The FAA Services Organization, AJR-B, collects and disseminates aeronautical and meteorological information and uses OASIS II to provide customized pre-flight and in-flight briefings to domestic and international general aviation inAlaska. These services are provided by Flight Service Specialists to pilots via phone or radio. Pilots can also access the information directly through online (Internet-based) web portals. Flight Service Specialists interpret weather and aeronautical data to provide pilots with weather briefings and flight planning services tailored for a particular flight. They also get the notification and alerts. Alternatively, pilots who access preflight information directly through a web portal are responsible for interpreting the weather and aeronautical information for their flight.

OASIS II provides the capabilities for acquiring and displaying textual and graphics weather products, emergency services, law enforcement, administrative and supervisory capabilities, flight planning and regulatory information and system maintenance functions. The FAA awarded the first OASIS contract in 1997 to modernize the aging hardware and software at up to 61 automated Flight Service Stations.

OASIS II is privately accessed and has no internal or external Uniform Resource Locators (URL). OASIS II is hosted locally at the 17 FAA Flight Service Stations in Alaska, and at the Anchorage Air Route Traffic Control Center (ARTCC). It is not a cloud-based solution. The computers communicate via the FAA's Operational (Ops) Network [FAA Telecommunications Infrastructure/Alaska Satellite Telecommunications Infrastructure (FTI/ASTI)].

OASIS II is used by FAA Air Traffic Control Specialists to provide weather briefing and flight planning information to general aviation pilots in Alaska. In addition to these services, OASIS II also provides information to support search-and-rescue services. OASIS II also process stolen aircraft alerts from law enforcement (LE) organizations Service B by messages regarding stolen aircraft. Flight Service Station Specialists use OASIS II to send responses to LE messages when the Flight Service has any contact with a stolen aircraft. System administration, supervisory, and system maintenance functions, such as database management and hardware/software status monitoring, are also provided.

OASIS II is an integrated computer-based system for the Alaska flight service facilities. It enables flight service specialists to provide weather briefing and flight planning assistance to general aviation pilots. OASIS II is provided as a contractor-managed service to FAA.The contractor owns the hardware and software and is responsible for second-level engineering, configuration management, depot maintenance, and Help Desk support to FAA operators and first-level maintainers. Contractor employees do not have access to the information in OASIS.

FAA regulations require flight plans to include the pilot's name, physical and mailing addresses, contact phone number, and aircraft location base, as well as emergency contact information (emergency contact name, phone number and address). This information is necessary to assist officials during law enforcement, search-and-rescue, and accident investigations. In the case of an emergency, the PII contained in OASIS II is shared by the FAA Flight

Services Quality Assurance Specialist upon formal request from law enforcement, search-and-rescue agencies, and/or the DOT/FAA organization responsible for accident investigations.

In the event of an accident, an Alaska Flight Service Specialist provides PII to emergency personnel using a telephone or OASIS II to generate a Service B message. If PII is provided by telephone, audio recordings are stored for 45 days. The Flight Plan is stored in OASIS II for 15 days. PII information given to emergency personnel is limited to the information the pilot provided as emergency contact information (emergency contact name, phone number and address). A pilot is not notified that their PII was released. It is understood by the pilot through training and flight plan filing requirements that their information will be shared with emergency officials in the event of an accident.

**PII Collected by OASIS II**

Flight plans require that pilots provide both PII and non-PII when flight plans are created. The information is collected when a flight plan is filed. It resides in OASIS II, but is only transmitted to law enforcement, search-and-rescue agencies, and/or the DOT/FAA organization responsible for accident investigations in the event of an accident. PII collected in the flight plan and stored in OASIS II consists of:

- pilot name,
- contact phone number,
- physical and mailing addresses,
- aircraft location base, and
- emergency contact information (emergency contact name, phone number and address).

Some pilots may elect to use their personal home phone number, personal cell number, email address, and personal home address in the flight plan. PII is entered into OASIS II manually by a FAA Flight Service Station Specialist when contacted by a pilot to file a flight plan.

## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template 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*[2].

### 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*



[2] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

*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.*

OASIS II is a System of Records subject to the Privacy Act because it contains pilot name, phone number, and address information. The authority for the collection of the information in OASIS is 49 U.S. Code § 44701 (C) All FAA Privacy Act SORNs can be found at https://transportation.gov/privacy. Records in the system are managed in accordance with FAA's DOT/FAA 847, *Aviation Records on Individuals*, Privacy Act system of records notice.[3] The OASIS does not provide automated notice and consent; however, FAA Flight Service Station Specialists are required to ask and receive a pilot's verbal consent before including the pilot's PII in the OASIS II flight plan. The recordings are specific to the facility and are not maintained by OASIS personnel or within the OASIS system boundary. These recordings are not maintained in accordance with N1-237-02-5. This records schedule authorizes the destruction of analog voice recordings after 15 day, and digital voice recordings after 45 days. The Flight Plan Form (OMB 2120-0026 / FAA Form 7233-1) is the only document containing a pilot's PII; no other pilot information is collected and stored in OASIS II.[4]

## Individual Participation and Redress

*DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in an FAA System of Records through the FAA 's Privacy Act/Freedom of Information Act (FOIA) procedures. As described in SORN DOT/FAA 847 and formalized in the Department's Privacy Act regulations at 49 CFR Part 10, FAA may exercise exemptions to the access provisions of the Privacy Act.[5] However, the FAA will review all Privacy Act requests on an individual basis and may as appropriate, waive applicable exemptions if the release of information to the individual would not detrimentally impact the law enforcement or national security purposes for which the information was originally collected or is subsequently being used.

Under the provisions of the Privacy Act, individuals may request searches of the OASIS II flight plan database to determine if any records pertain to them by sending a written request directly to the OASIS II Program Office that contains name of requestor, verification information, and information regarding the request. The FAA does not allow access through either the Internet or Intranet to the information stored in the OASIS.

As described in DOT/FAA 847, individuals with questions about privacy and OASIS II should contact the FAA directly. For inquiries, a letter should be sent to the System Manager at the address specified below:

Stephen C. Ryan
Flight Service Program Operations
Federal Aviation Administration



[3] *See* - http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28237.pdf (75 FR 6884, November 9, 2010)
[4] *See* - https://www.faa.gov/documentlibrary/media/form/faa_form_7233-1_7_31_17.pdf
[5] *See* - https://www.law.cornell.edu/cfr/text/49/appendix-to_part_10

800 Independence Avenue, SW
Washington, DC 20591

Individuals with concerns about privacy in regard to OASIS II may also email the FAA Privacy Officer via the contact information provided in the privacy policy on the FAA's web site (www.faa.gov/privacy).

## 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 its collects, uses, maintains, or disseminates PII.*

The FAA is responsible for maintaining records on individuals in connection with FAA's oversight and enforcement of safety regulations as described in DOT/FAA 847. To that end, OASIS II collects information necessary to identify individuals for search and rescue and accident investigation 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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.*The

DOT is requesting the minimum amount of information necessary to meet the statutory requirements that OASIS II is designed to fulfil. OASIS II will collect and retain only the following information from the: first name, last name, basic contact information, and flight plan information (as described previously in the Introduction & System Overview section).

OASIS II records are scheduled under National Archives and Records Administration (NARA) Schedule Reference Number N1-237-02-5, dated May 29, 2002. Flight plans containing PII data in OASIS II are retained for 15 days only. Flight plan data is used for law enforcement, search-and-rescue, and/or accident investigation purposes only. The flight plans containing the PII are stored on the OASIS II flight data server and are required to be retained for 15 days. However, the voice recordings are stored in the OASIS system. Flight plans older than 15 days are deleted or overwritten by new flight plans generated within OASIS II.

Unless there is a formal data request from law enforcement personnel, the information is needed for a search and rescue situation, or an accident investigation, the PII contained in the OASIS flight plan is not used by other applications or systems or included in any reports.

## 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 use of records contained in OASIS are limited to search and rescue and accident investigation purposes and the routine uses identified in DOT/FAA 847. Specifically, records are shared by the FAA Flight Services Quality Assurance Specialist upon formal request from law enforcement, search-and-rescue agencies, and/or the DOT/FAA organization responsible for accident investigations. The process for requesting, controlling, and releasing the information is identified in the DOT regulations 49 CFR Part 10. Compliance with these regulations is strictly enforced.

## 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 PII required in the OASIS II flight plan is provided verbally by the pilot and entered into the system by the Flight Service Station Specialist. Voice recordings (VRs) of pilot-specialist interaction are stored for 45 days. The VR system is independent of OASIS II. When flight plan PII is changed, OASIS II maintains a copy of the flight plan and records to which Flight Service Station Specialist made the changes. OASIS II stores flight changes to the flight plan as amended flight plans. Amended flight plans can be retrieved from the OASIS II database by the Flight Service Station Specialist, if required. Accuracy of the PII data is dependent on both the pilot and the Flight Service Station Specialist. A Flight Service Station Specialist can retrieve stored VRs to review pilot information; however, there is no means available to validate the accuracy of the data. The process for filing a flight plan does not require the pilot to provide official identification...

## Security

*DOT shall implement administrative, technical, and physical measures 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. OASIS II received its authority to operate on July 24, 2014 after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A) process (formerly known as the certification and accreditation [C&A]). Access to OASIS II is limited to authorized personnel only. Access to FAA facilities is restricted using a combination of physical and logical access controls (e.g. fences, badge/card readers with keypads, visitor control, closed-circuit TV). OASIS II complies with Federal Information Security Management (FISMA) requirements. OASIS II is assessed annually to ensure FISMA Security controls are applied and the National Institute of Standards and Technology best security practices are implemented. FISMA requires that specialized security controls be applied to safeguard PII and other sensitive data by not making data available to unauthorized persons. The FAA does not allow access through either the Internet or Intranet to the information stored in the OASIS II. Data stored in the OASIS Master Contact Database is encrypted. In addition to physical and logical access control, OASIS limits access to PII according to job function.

## 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 1370-121, FAA Information Security and Privacy Program and Policy. FAA Order 1370-121 implements the various privacy requirements of the Privacy Act of 1974, as amended (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), FISMA, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. In addition to these, 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, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of OASIS relative to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

OASIS II is assessed annually to ensure FISMA security controls are applied and the National Institute of Standards and Technology (NIST) best security practices are implemented. FISMA requires that specialized security controls be applied to safeguard PII and other sensitive data. The FAA does not allow access through either the Internet or Intranet to the information stored in the OASIS II. In addition to physical and logical access controls, OASIS II limits access to PII according to job function.

## Responsible Official

Stephen C. Ryan
Manager, Flight Service In-Service Management, AJR-B2
Federal Aviation Administration

## Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer