U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Swim Cloud Distribution Service (SCDS)

Responsible Official

Kristin Cropf
Email: kristin.m.cropf@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) System Wide Information Management (SWIM) program office provides the network-centric infrastructure that enables FAA programs to share information with aviation stakeholders. SWIM offers improved interoperability using industry-supported standards, proven infrastructure technologies, and FAA data sharing governance as information services. The FAA uses the SWIM Cloud Distribution System (SCDS) to share information with aviation stakeholders outside of the FAA for non-operational use such as to academia for research, to aviation entities for business analysis purposes, and to the public.

In accordance with E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because the SCDS collects Personally Identifiable Information (PII) from members of the public including first and last names, company names, phone number, and email addresses when an SCDS account profile is created. SCDS also collects this information from FAA employees and contractors for account profiles.

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 FAA Air Traffic Organization's SCDS promotes information management and exchange technologies to ensure that SWIM-enabled systems and users have access to information to improve the speed, efficiency, and quality of distributed decision-making across the National Airspace sharing service externally. SCDS leverages cloud technologies to deliver an information distribution solution that provides data from the National Airspace System (NAS) to external consumers for non-operation use such as to academia for research, to aviation entities for business analysis purposes, and to the public.

SCDS is a publicly available, cloud-based infrastructure dedicated to providing near real-time SWIM data to the public via Java Message Services (JMS) through the FAA Public Cloud. SCDS enables external consumers[2] to register and subscribe to SWIM content using an automated onboarding process facilitated via the Consumer Portal using the first and last name, company name, and email address they provided the FAA via https://data.faa.gov. The SCDS Messaging Service receives SWIM content originating from the FAA Telecommunications Infrastructure NAS Enterprise Security Gateway (FTI NESG)[3] using the existing process utilized by SWIM external consumers. This data has been approved for release to the public by the NAS Data Release Board (NDRB).[4] Information accessible to the public through SCDS includes terminal weather, aeronautical information, flight information, flow information, terminal surveillance, and continental United States (CONUS) weather products. No PII can be accessed by the public through this system.

[2] Consumers are considered to be individuals that request data from the SCDS; users are considered to be individuals who are involved with the operation of the system.
[3] The FAA sends its System Wide Information Management (SWIM) flight plan, aeronautical and weather data to the SWIM cloud Distribution System (SCDS) via a one-way VPN connection from the NAS Enterprise Messaging Service (NEMS) at the NAS Enterprise Security Gateway (NESG) to SCDS.
[4] Release of NAS data is governed by FAA Order 1200.22E, *External Requests for National Airspace Systems (NAS) Data*.

SCDS provides a web management portal for users to request and manage access to SWIM subscriptions.

- To access SCDS, an individual must first register for FAA data access at https://data.faa.gov. This process and the associated collection of PII is outside of SCDS.
- Consumers then go to the SCDS Portal and provide their first and last name, company name, and email address that was used to register at https://data.faa.gov previously. Consumers provide a password to establish an account.
- Consumers then request access to available SWIM data. The Consumer agrees to the SWIM Terms and Conditions externally to SCDS; the request then must be approved by the SCDS approver.
- Once an account is approved, the Consumer connects to SCDS message broker via a Transport Layer Security (TLS) protocol connection to receive SWIM data.
- Consumers may view their content subscription requests pending, subscription approvals, connection details, content consumption metrics, download a jumpstart kit, use the message data viewer, and review their user account information.

Once a Consumer sets up an SCDS account on the self-service portal, they can register for SWIM data access via the FAA SWIM program office. All access is password protected.

- SCDS Portal: https://portal.swim.faa.gov/
- Accounts Portal (SSO): SWIFT Portal - Sign In (faa.gov)

Members of the public (Consumers) access the Accounts Portal to manage their account profile and SWIM content subscriptions. The FAA presents a Privacy Act Statement at the SWIFT Portal sign-in page. Consumers establish an account within the Consumer Portal and upon approval by the SCDS Privilege User group, may request access to publicly available SWIM data services. These services provide additional identity management services for SCDS to ensure the identity of the users is validated. Google Authenticator is used for two factor authentication for admin user roles. KeyCloak is a part of SCDS. It was purchased to maintain user credentials (username, password). Solace is a commercial of the shelf (COTS) product also apart of SCDS. It is an enterprise message product that utilizes Java Messaging protocol used by SCDS to distribute SWIM data. Most FAA internal network data is sent through FTI. Data is pulled from FTI to SCDS.

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[5], 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[6].

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 deploys the following methods to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains PII within SCDS. The Department of Transportation (DOT) has published an existing Privacy Act System of Records Notice SORN, DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) to provide notice to the public of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about an individual that may be collected. As noted above, a Privacy Act Statement is presented at the SWIFT Portal sign-in page. In addition, the publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency for SCDS.

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.

SCDS collects registration information directly from Consumers through the SCDS website portal. Consumers provide their first and last name, company name, phone number, and email address that was previously used to register at https://data.faa.gov. Consumers also create a password to establish an account. Once the account is established, Consumers may

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

access their information via the self-service portal to make any changes necessary to their profile information.

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 this system may inquire in person or in writing to:

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

The following information must be included in the request:

- 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 this system should make their requests in writing, detailing the reasons for why the records should be corrected to the following address:

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

Purpose Specification

DOT should (i) identify the legal basis 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 PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

SCDS is authorized under Title 49 United States Code (U.S.C.) § 40101. The purpose of SCDS is to provide data from National Airspace System (NAS) to external consumers for non-operations use such as to academia for research, to aviation entities for business

analysis purposes, and to the public. To support this purpose, SCDS uses the following business processes and corresponding collections of PII:

- To establish a profile, SCDS collects and maintains: first and last name, company name, phone number and email address.
- For identification purposes, SCDS relies on the first and last name, company name, and email address.
- To establish access and data subscriptions, SCDS uses email addresses and passwords from members of the public, FAA employees, and FAA contractors.
- First and Last name, email and company name is captured in the application's audit logs.

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.

SCDS collects the minimum amount of PII necessary to enable external consumers to register, maintain a profile, and subscribe to SWIM content using an automated onboarding process facilitated via the Consumer Portal. The onboarding process utilizes the first and last name, company name, and email address used with https://data.faa.gov. Consumers provide a password to establish an account. The Consumer Portal is a web-based interface for external consumers to manage their account profiles and service subscriptions.

SCDS records containing terminal weather, aeronautical information, flight information, flow information, terminal surveillance, and CONUS weather products are maintained in accordance with General Records Schedule 5.2, *Transitory and Intermediary Records* are destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

SCDS system records, such as an audit log of users accessing the system, are maintained under General Records Schedule 3.2: *Information Systems Security Records, Item 030: Systems Access Records.* These records are temporary and are destroyed when business use ceases, 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.

SCDS provides data from National Airspace System (NAS) to external consumers for non-operations use such as to academia for research, to aviation entities for business analysis purposes, and to the public. To do so, FAA collects PII from individuals, as noted in the "Purpose Specification" section above. FAA does not use this information for any other purpose.

The sharing of user account information in the SCDS system is conducted 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).

FAA promotes data quality by collecting SCDS registration, profile, and login information directly from the individual. Because FAA collects this information directly from the individual, the information is assumed to be accurate. SCDS also allows individuals to log into their profiles at any time to edit their information, as needed.

As noted in the Security section below, FAA employs reasonable controls to reduce the risk of unauthorized access and modification of SCDS data, including access controls.

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.

SCDS has gone through an assessment of risk and received an authority to operate, and continuous monitoring is used to ensure continued technical protections. Specifically, SCDS takes the following steps to safeguard PII, including but is not limited to identification and authentication of two-factor authentication, physical security, access controls based on roles and permissions on the user profile, and encryption of data at rest. Access to the system can only be achieved by an authorized user connected to the SCDS environment, and the software and operating system have extensive logging. The infrastructure that hosts the SCDS employs firewalls, and intrusion detection/prevention systems, and the system is routinely scanned for vulnerabilities.

Accountability and Auditing

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

FAA Order 1370.121B, *"FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with SCDS are given clear guidance about their duties related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy training awareness training, as well as FAA Order 1370.121B. The FAA will conduct periodic privacy compliance reviews of SCDS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Kristin Cropf
System Owner
Program Manager Air Traffic Organization

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: 2024.03.27 10:33:47 -04'00'