U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Knowledge Services Network (KSN)

Responsible Official

Mark Frisk
Email: mark.frisk@faa.gov
Phone Number: 412-304-7883

Reviewing Official

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

Executive Summary

The Federal Aviation Administration's (FAA) Knowledge Services Network (KSN) is an enterprise-level service that allows users to design, build, and manage their own collaborative work sites using SharePoint. The KSN environment supports over 500 unique site collections and tens of thousands of individual content sites for a user base of over 50,000 FAA-named users. In accordance with the E-Government Act of 2022, this Privacy Impact Assessment (PIA) is being conducted because the KSN environment maintains records that could include personally identifiable information (PII) about members of the public.

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

The KSN virtual workspace environment structures daily work into managed storage areas and categories such as document libraries, announcements, events, contacts, discussion boards, and miscellaneous lists. Within these areas, users can share and collaborate with other users on their daily work activities.

Personal Identifiable Information (PII) is present in the KSN environment, and includes, but is not limited to, contact information for employees and contractors, airmen, aircraft owners, air carriers, and other entities; certificate numbers and type; aircraft information; aircraft registration; citizenship; and date of birth information. All PII on the KSN environment must be encrypted per Federal Information Processing Standard (FIPS) 140-2 methodology in accordance with FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*. While the KSN environment may be used as a repository for official federal records[2], official Privacy Act Systems of records are not permitted to be maintained in the KSN environment and must be maintained in the appropriate official recordkeeping system. Privacy Act Systems of records specifically include records about individuals that are maintained in a federal information technology system (or other systems), which are retrievable by a personal identifier, such as an individual's name or phone number.

Users of the KSN environment include Department of Transportation/ Federal Aviation Administration (DOT/FAA) employees, contractors, and members of the public, such as external stakeholders from federal, state, and local governments, academia, and private industry who collaborate with the FAA. DOT/FAA employees/contractors authenticate to KSN with their Personal Identity Verification (PIV) cards via an exchange of name and FAA email address with Active Directory (FAA Directory Services). For DOT/FAA employees, KSN also receives via the Employee Information System (EIS), MyProfile[3],

[2] Pursuant to 44 U.S.C. 3301, a federal record includes "all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them."

[3] MyProfile is an employee information system that captures all employee information in one place.

information such as user's name, FAA email address, profile ID, desk location, business fax number, line of business, mailing address/building name, work phone number, contractor business name as well as other organization information, to maintain profile information for users.

External Users do not have PIV cards and must authenticate with a username and password. External user accounts must be created by a Government Responsible Individual (GRI), who is an FAA employee or contractor with an FAA domain account, who creates a username and temporary password for the external user, which they provide to the external user via email. No other information is maintained in the KSN about the external user. The FAA employee/contractor who provisions an external account is responsible for vetting the external user. The GRI must perform a yearly audit of all users and permissions and ensure that the site collection is properly protected and accessible only to those with a need to know.

The KSN environment allows a GRI to set up and administer individual KSN sites and invite other users. On an annual basis, the GRI is required to sign an updated KSN Rules of Behavior (ROB), which details their responsibilities regarding site collection management, the storage of PII, storing sensitive unclassified information (SUI), and their recordkeeping responsibilities. This ROB establishes the following, regarding how the GRI must manage PII:

- Implementing and ensuring that appropriate controls and mechanisms are in place to protect PII/Sensitive PII (SPII).

- Ensuring that all PII/SPII is properly handled as outlined in the Office of Management and Budget (OMB) guidance, *M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.

- Ensuring that all PII/SPII is protected in accordance with applicable statutes and regulations, including, but not limited to, the Privacy Act, the E-Government Act, the Department of Transportation Privacy Act regulations at 49 C.F.R. part 10, and internal FAA and DOT policy, including but not limited to FAA Order 1370.121B or its successor, *FAA Information Security and Privacy Program & Policy*.

In addition to the ROB, the KSN provides a variety of other governance and policy documents for users to review, including the KSN Operating Model, which includes data policy, credential creation policy, and other operational guidance.

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[4], 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[5].

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 employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII within the KSN. Information about the KSN environment is provided to FAA employees and contractors via broadcast communications. The FAA also requires all employees and contractors to take annual security training, which includes information about data protection responsibilities. FAA's KSN sites are accessible to a limited number of members of the public, such as specific aviation community members.

KSN access-related records about FAA users are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002). KSN is not a Privacy Act system of records and users are not permitted to maintain Privacy Act systems of records in the environment. Any copies of Privacy Act records maintained in KSN sites are used and disclosed in accordance with the applicable SORN.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

[4] https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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.

FAA users receive notice of proper use of government systems in the form of training, instructions, Rules of Behavior, KSN governance documents, and FAA Order 1370.121B, *FAA Information, Security and Privacy Program & Policy*.

While the KSN environment may be used as a repository for official records, official Privacy Act Systems of records are not permitted to be maintained on the KSN and must be maintained in the appropriate official recordkeeping system. Privacy Act Systems of records specifically include records about individuals that are maintained in a federal information technology system (or other system) and which are retrievable by a personal identifier, such as a name.

The Privacy Act affords individuals the right to request and receive their own Privacy Act records. Individuals wishing to access their KSN user account records may inquire in person or in writing (by email or mail) to:

Email: privacy@faa.gov

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

The written request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

• Signed attestation made under penalty of perjury stating your identity

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 KSN environment is integral to the operations of the FAA in furtherance of its responsibilities to ensure aviation safety under 49 U.S.C. § 40103. The KSN environment provides a mechanism for the FAA workforce to collaborate on various projects and initiatives in a secure environment. PII present in the KSN environment includes, but is not limited to, contact information for employees and contractors, airmen, aircraft owners, air carriers and other entities; certificate numbers and type; aircraft information; aircraft registration; citizenship; and date of birth information. Account information (name, FAA email address, work phone number, username/password, contractor business name, and business address) is maintained about users. The PII contained in these records is used for FAA business purposes only and is necessary for the FAA to perform its aviation safety, policy, and personnel management activities.

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.

The FAA collects and maintains only the minimum amount of information necessary for the FAA to perform its aviation safety, policy, and personnel management activities. Official records maintained within the KSN are subject to approved record retention schedules. GRIs are instructed to work with their Line of Business Record Management Officer regarding record retention policies for records maintained on the KSN. Due to the variety of types of records present in the KSN environment, retention periods vary depending on business needs for the information. However, GRIs are responsible for ensuring copies of records are destroyed once no longer needed for business purposes.

Finally, as noted above, official Privacy Act System records are not permitted to be maintained in the KSN environment and must be maintained in the appropriate official recordkeeping system.

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 FAA specifically limits the exfiltration of PII data from KSN in several ways. The KSN performs scans to restrict large groups of users from being able to access data (i.e., no groups for "All FAA" users, "All Domain" Users, etc.). Additionally, all GRIs are required to annually review and sign the ROB, which requires the GRI to protect PII as required by FAA statutes, regulations, and requirements. The KSN Support Team has submitted a request to the Information Security & Privacy Service's, Risk Management Branch, to begin performing routine data loss prevention scans, to ensure that data elements such as Social Security Numbers (SSN), credit card numbers, and sensitive security information (SSI) are not present within the KSN environment.

In addition, while the KSN does not maintain official Privacy Act systems of records, to the extent copies of Privacy Act records are included in a KSN site, GRIs are responsible for ensuring that these copies are maintained and disclosed only in accordance with the Privacy Act and the system of records notice that applies to the record. Within FAA, Privacy Act records are shared only with those who have a business need to know the information. GRIs and their site collection users are responsible for ensuring that user permissions for records containing PII are restricted to those within the FAA workforce who have a need to know. Furthermore, profile and login PII collected by the FAA is used only as specified by the Department's system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records*. In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this 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 approved investigations 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 negation 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; and
- To other government agencies where required by law.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses."

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).

In most cases, employees have direct control over their KSN profile information and may edit it to maintain its accuracy at any time. The accuracy of other information maintained in the KSN environment can be corroborated via other FAA systems. The individual user within the system will need to determine accuracy based on business knowledge and need. Moreover, the collaborative nature of KSN provides opportunities for those working together on a document, for example, to make changes to address any inaccuracies concurrently. Errors in copies of records must be addressed within the source system; however, to the extent an error in the source system is identified, the record will likewise be corrected in the KSN if appropriate. Privacy Act System records are not permitted to be stored on the KSN and must be maintained in the appropriate official recordkeeping system. Privacy Act System records specifically include records about individuals that are maintained in an information technology system (or other system) and which are retrievable by a personal identifier.

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 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 FISMA and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy",* FAA Order 1600.75, *Sensitive Unclassified Information Policy (SUI)*, FAA Order 1375.1F, *FAA Data and Information Policy* and FAA Order 1350.14B, *Records Management Policy*" and NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* dated January 22, 2015.

The KSN environment implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of least privilege is used to grant access to FAA federal employees and contractors, and user actions are tracked

in the KSN audit logs. GRIs must also provide guidance to users on where to store specific types of information within the site collection to ensure the content is properly protected, as well as restrict access to all PII stored within the site collection to only those persons with a business need to access the information. The KSN Program also performs an annual review of security permissions within their site collection to ensure all content is properly handled and protected.

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 Information Security and Privacy Service (AIS), Security Governance Division is responsible for the administration of FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121B defines 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), the *Federal Information Security Management Act (FISMA)*, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other 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 on 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. In addition, staff are required to acknowledge understanding of the FAA Privacy Rules of Behavior (ROB) and agree to them before being granted access to FAA information systems. The DOT and FAA Chief Privacy Offices will conduct periodic privacy compliance reviews of the KSN relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Mark Frisk
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: 2024.03.26 10:39:17 -04'00'