Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 415
System Name: Federal Service Desk (FSD)
CPO Approval Date: 2/7/2023
PIA Expiration Date: 2/6/2026

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Prasanthi Narra

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Federal Service Desk (FSD)

B: System, application, or project includes information about:

FSD provides contact center services and related state-of-the-art technical tools so that the customer experience is one that enables customers, including federal employees, contractors, the public, to easily perform the work or seek the information for both the private and public sectors. As such, during support operations,

FSD collects and stores contact information, including usernames, email addresses, and phone numbers primarily to communicate with the user about the status and resolution of their ticket/issue when doing business with the U.S. government.

C: For the categories listed above, how many records are there for each?

Approximately 2.1 million records.

D: System, application, or project includes these data elements:
The FSD systems and applications include Name and other biographic, demographic or biometric information, Contact information, and User and online information.

Overview:

The primary purpose of the Federal Service Desk is to provide services to support users of current and future IAE applications. This support is to assist users in all Department of Defense and Civilian Departments and Agencies in the Federal Government, as well as all other users of the IAE. FSD provides Tier 1 and Tier 2 service request Support for all IAE applications, Tier 2 service request Support for SAM, Development, maintenance and enhancement of Tier 0 (user self-help) materials and the IAE FSD Portal, Continuity of Operations support, deployment and maintenance of the call center management application solution, Interactive Voice Response (IVR) System, and Service Request Management System, as well as, to provide surge support.

To achieve the functionality described above both cloud services (ServiceNow, NICE/InContact, and Login.gov) and privately-owned systems will be integrated using industry standard protocols. More specifically the integration between ServiceNow and NICE/InContact is achieved using REST/SOAP while the integration between ServiceNow and Login.gov is supported via OAuth.net (or SAML 2.0). All communication between the systems will align with FIPS 140-2 and is encrypted vis secure HTTP. ServiceNow and NICE/InContact both reside, within FedRAMP accredited cloud services (ServiceNow resides at FedRAMP High and NICE/InContact resides at FedRAMP Moderate).

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c), following GSA 2180.1 CIO P GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
New SORN required

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
Data is retrieved by FSD personnel by searching against email address or phone number.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
System records are retained and disposed in accordance with GSA records maintenance and disposition schedules and 1820.1 OAS P GSA Records Management Program, the requirements of the Recovery Board, and the National Archives and Records Administration (NARA).

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
FSD collects necessary information from individuals and entities seeking to do business with the U.S Government. The collection of names, email addresses, and phone numbers is needed to accurately associate support requests and ticket management activities with the correct unique user. Calls may be monitored or recorded for quality assurance purposes. Non-PII cannot be used for these purposes as it does not provide adequate correlation of support requests for a unique user.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
FSD services are provided using cloud resources authorized at FedRAMP Moderate or higher. Access to FSD systems requires multifactor authentication, which is provided and managed by Login.gov. Access to individuals' information is protected through role-based access controls. System API calls into the FSD ticketing system (i.e., SAM.gov ticketing integration) require basic authentication. FSD has implemented technical operational management control to safeguard system and data and to maintain the system security.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
No, FSD systems do not locate or monitor any individual for any purpose.

3.5 What kinds of report(s) can be produced on individuals?
FSD does not produce any reports on individuals for the purpose of monitoring (e.g., cross-device tracking). Reports on individuals are provided at the request of GSA and are specific to user activity (i.e., login, ticket submission and audit of internal FSD performance of customer service activities, as required for GSA.)

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
No, FSD does not generate any reports, there will be no need for the de-identifier.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
GSA will not share any information collected with external parties.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?
The FSD system relies on Login.gov for user authentication services. As a part of the authentication transaction, FSD also receives email addresses of individuals from Login.gov. The information is provided over a federated connection and protected using a TLS 1.2 encrypted connection. FSD information is not shared with non-Federal agencies. Additionally, SAM.gov api integration making use of system account setup in SAM.gov and apiKey utilization for invoking SAM.gov apis. The RPA bots, that are going to be set up for attachment backups, are making use of FSD.gov frontend only. The RPA bots,that are set up for EVS ticket resolution, are making use of the SAM.gov Generic Incident apis which in turn calls FSD apis.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
When collecting contact information, including first name, last name, email address and phone number during contacts with the FSD, FSD Business Rules and Standards require FSD Associates confirm spelling of each data element, for accuracy. Users can work with FSD Associates to maintain accuracy and completeness of information in the ticketing system.

Because FSD relies on Login.gov for management of identity services and authentication, FSD is not able to maintain user information provided by Login.gov.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
FSD manages system and data access through role-based access controls. GSA requires all FSD personnel supporting the system to undergo background investigations and signing of Rules of Behavior. Non-FSD personnel (i.e., customer users) are required to authenticate through Login.gov when accessing FSD for ticket status or creation and are limited by system restrictions to only viewing and adding comments to their own tickets.

6.1b: What is the authorization process to gain access?
FSD manages system and data access through role-based access controls. GSA requires all FSD personnel supporting the system to undergo background investigations and signing of Rules of Behavior. Non-FSD personnel (i.e., customer users) are required to authenticate through Login.gov when accessing FSD for ticket status or creation and are limited by system restrictions to only viewing and adding comments to their own tickets.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/28/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Physical security for FSD systems and applications is provided by the FedRAMP Authorized Cloud resources. Systems and applications are also secured through federated identity management using Login.gov, multifactor authentication requirements for all users, role-based access controls, and encryption of data at rest and in transit.

The FSD Contact Center API server connections require account authentication to generate an expiring token and then token authentication based on a created API application and user account in the system. API calls must be made over REST with TLS 1.2 or greater. While voice is being captured in real-time (i.e. spoken over the phone) it is not encrypted. Once the call ends and is stored, then the call recording is encrypted at rest and in transit. The database containing call history, with the ANI, is encrypted at rest with always-on encryption (AES 256 FIPS 140-2)

Managerial controls are provided for FSD systems and applications include required background checks for FSD support personnel and privileged users. Security and privacy training, as well as signed Rules of Behavior are required for FSD personnel prior to accessing systems and applications. Application training and ongoing training through GSA-approved Knowledge Articles (KAs) are provided to FSD support personnel. FSD also provides Incident Response, Audit, and Reporting to support security of systems and applications.

FSD has also implemented technical, operational and management controls to safeguard the information system and maintain the security posture.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
FSD has developed and maintains an Incident Response Plan for responding to suspected and confirmed security incidents, including breaches of PII.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

FSD customers do have the ability to consent or decline any information. However, FSD customers who decline to provide contact information will be limited in the amount of assistance that can be provided by the FSD services. For example, this includes limitations on ability to assist with issues requiring information to support escalations.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?
Users cannot access their own information.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
FSD trains IAE Government and support contractor staff on the FSD Service Request Management System. This includes initial system training, and user training for new users. FSD provides Information Security Awareness and Training Records to GSA ITSS ASSIST System.

FSD maintains Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1). FSD provides the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT 3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
GSA requires privacy and security training for all personnel and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act.
All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. GSA takes automated precautions against overly open access controls. GSA's CloudLock tool searches all GSA documents stored on the Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.