




Instructions

Privacy Impact Assessment (PIA)

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

00 Default Layout

Workflow Status:

99 Workflow Complete

PIA

General Information

PIA ID:	PIA-357	PIA Status:	Completed
Authorization Package (System Name):	Federal Service Desk (FSD)	This is a RPA:	No
Assessment Date:	2/3/2022	Is Latest:	Yes
FISCAL Year:	2022	PIA Required (From Authorization Package):	Yes
Final FISCAL Year:	2022	PIA Expiration Date:	2/3/2023
		Final PIA Expiration Date:	2/3/2023

Override / Reopen Explanation

Override FISCAL Year:

Override PIA Expiration Date:

Reopened Explanation:

Other Stakeholders

Stakeholders (not in Approval Process)

System Owner (SO): Romero, Antonio

Authorization Official: Samant, Sagar S

System Owner (eMail)

Name (Full)

Antonio Romero

Authorization Official (eMail)

Name (Full)

Sagar Samant

PIA Overview

A.System Name:	A. System, Application, or Project Name:	Federal Service Desk (FSD)
B.Includes:	B. System, application, or project includes information about:	<p>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,</p> <p>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.</p>
C.Categories:	C. For the categories listed above, how many records are there for each?	Approximately 2.1 million records.
D.Data Elements:	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 Federal Service Desk (FSD) serves as the Tier 1 help desk for SAM.gov. The primary purpose of the FSD is to provide services to support users of current and future IAE applications. This support assists users in all Department of Defense and Civilian Departments and Agencies in the Federal Government, as well as all other users of the IAE. The 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.

FSD collects PII through either direct interaction with Help Desk agents or by automated system processes. 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.

FSD Help Desk agents collect information from callers during the customer contact for support. For example, the customer contact is asked to provide their First Name, Last Name, Email address, contact phone number, and DUNS number to create a new contact record or to confirm an existing record or support request.

To provide support, the FSD maintains existing PII data (first name, last name, email address, and phone number) and collects email addresses, phone numbers, to associate requests with specific customers. Users provide this information by connecting through external systems through Login.gov or directly when requesting support over the phone or using web chat from the FSD.gov website. FSD systems maintain this information to associate customers with their related support requests.

Automated collection occurs when the caller's phone number is provided automatically to the Interactive Voice Response (IVR) system through the Automated Number Identification (ANI), a feature of the telecommunications network. The phone number is then used to lookup customer information from the existing ticketing database using an FSD Application Programming Interface (API). The name associated with the caller's number allows the caller to confirm their identity before connecting to a Help Desk agent for support.

Automated collection can also occur when users access FSD after authenticating through login.gov. FSD connections received through login.gov will create the user account automatically using their email address. The user information is stored in the user's account in the FSD ticketing system.

PIA-0.1: Is this a new PIA or Recertification request? New PIA

PIA-0.1Changes: If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA-4.3	Henry, Jacquelyn F	1/12/2022	What is the other source?	

1.0 Purpose of Collection

PIA-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).
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	New SORN required
	PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-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. SORN is N/A until PIA has been completed and finalized.
PIA-1.2b:	Explain why a SORN is not required.	
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.	
PIA-1.4:	What is the records retention schedule for the information system(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

PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2.1 Explain:	If not, please explain.	

3.0 Data Minimization

PIA-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.
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3.2Explained:	If so, how will this data be maintained and used?	
PIA-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.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3.4Explain:	Please elaborate as needed.	No, FSD systems do not locate or monitor any individual for any purpose.
PIA-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.)
PIA-3.6:	Will the data included in any report(s) be de-identified?	No
PIA-3.6Explain:	If so, what process(es) will be used to aggregate or de-identify the data?	
PIA-3.6Why 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

PIA-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
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	None
PIA-4.2How:	If so, how will GSA share the information?	GSA will not share any information collected with external parties.
PIA-4.3:	Is the information collected:	Directly from the Individual From Another Source
PIA-4.3Other Source:	What is the other source(s)?	
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes
PIA-4.4Who How:	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.
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	<p>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.</p> <p>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.</p>
-----------------	--	--

6.0 Security

PIA-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.
PIA-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.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	11/25/2020

<p>PIA-6.3:</p>	<p>How will the system or application be secured from a physical, technical, and managerial perspective?</p>	<p>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.</p> <p>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)</p> <p>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.</p> <p>FSD has also implemented technical, operational and management controls to safeguard the information system and maintain the security posture.</p>
<p>PIA-6.4:</p>	<p>Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?</p>	<p>Yes</p>
<p>PIA-6.4What:</p>	<p>What are they?</p>	<p>FSD has developed and maintains an Incident Response Plan for responding to suspected and confirmed security incidents, including breaches of PII.</p>

7.0 Individual Participation

PIA-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.
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7.1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
PIA-7.2:	What are the procedures that allow individuals to access their information?	Users cannot access their own information.
PIA-7.3:	Can individuals amend information about themselves?	No
PIA-7.3How:	How do individuals amend information about themselves?	

8.0 Awareness and Training

PIA-8.1:	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	<p>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.</p> <p>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.</p>
-----------------	--	---

9.0 Accountability and Auditing

PIA-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.