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: 371
System Name: Federal Supply Service 19 (FSS19)
CPO Approval Date: 6/2/2022
PIA Expiration Date: 6/1/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Mark Zenon

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Federal Supply Service 19 (FSS19)

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

Sub System Name/Module: FSS-19 PR Module
PII data elements: TIN(Tax Identification Number) or SSN(Social Security Number)
PCI DSS data: None

C: For the categories listed above, how many records are there for each?
Sub System Name/Module: FSS-19 PR Module
PII data elements: TIN(Tax Identification Number) or SSN(Social Security Number)
PII Record Count: ~4.2M

D: System, application, or project includes these data elements:
Sub System Name/Module: FSS-19 PR Module
PII data elements: TIN(Tax Identification Number) or SSN(Social Security Number

Overview:

FSS-19 PR Module
Purpose FSS-19 is a collection of mainframe Work Flow Language (WFL) scripts that run on the Clearpath Unisys mainframe for the principal data processing of the FSS-19 System. Many of these modules work with other FSS-19 sub-applications to provide the data interaction functionality for user interfaces (such as FSS On-line, eFSSOnline, etc.)
FSS-19 Modules are implemented via the WFL scripts. The FSS-19 PR (Procurement) module automatically processes orders from the OP module (Purchase Orders) and sends all Federal Acquisition Service (FAS) Awards data to Federal Procurement Data System (FPDS). Also provides support to maintain Contract Writing System, maintain Industrial Funding Fee (IFF) Sales Records, and generate Multiple Award Schedule (MAS) and IFF Management Reports.
Description of PII FSS-19 processes sensitive data including Financial information and PII. As FSS-19 processes TIN for payees and payees can be individuals, some SSN information would be included, which is PII (in the PR module). Financial information can include vendor financial account information and agency payment, budget, and AR data in the PR, OP, PM, and Finance modules. Other sensitive information includes contract data, proprietary vendor information, and contract performance data in the PR module.
Handling of PII (Collection, Use & Destruction) FSS-19 PR module uses the DMS II database on the Unisys plus mainframe hosted in the Clearpath data center. It relies on the Clearpath Hosting Center for many inherited or hybrid security controls.
Covered under SORN ID GSA/GOVT-9 for SAM (System Awards Management).

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
1. The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

2. Agreements with external agencies are listed in the following table: FSS-19 Subsystem/Module External Agency Agreement Type (ISA, MOU/PBA)

FSS19 DLA PBA FSS19 FEDLOG - outgoing. MOU

FSS19 USPS - incoming to GSA ISA

FSS19 USCG ISA

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?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
FSS 19 PR Module: SORN ID GSA/GOVT-9 for SAM (System Awards Management).

1.2b: Explain why a SORN is not required.

FSS-19 in covered under the SAM SORN

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.
Not applicable. Information is collected by the sam.gov system and relies on that system for any approvals.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
There is no records retention schedule specifically for FSS-19. FSS-19 will follow the records schedules for enterprise IT systems outlined in GRS 03.1/020 and GRS 03.2/010 GRS 03.1/020 Information Technology Operations and Maintenance DAA-GRS-2013-0005-0004. Information technology operations and maintenance records. Information Technology Operations and Maintenance records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure. Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. GRS 03.2/010 Systems and Data Security Records. DAA-GRS-2013-0006-0001 Systems and data security records. These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes to analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls though out the life of the system.

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? No

2.1 Explain: If not, please explain.
NA. The collection of PII is collected outside of the application via application programming interface. The vendor is notified via the registration site sam.gov

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The FSS-19 set of applications, supports government wide contracts with commercial companies that provide access to millions of commercial products and services at fair and reasonable prices to the government. The application makes buying easy and efficient with the use of modern technology to connect government buyers and industry. The collection of PII is critical to the mission for vendor identification, notification and payment collection purposes. For more details see Overview section

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?
NA. No new data is aggregated

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
NA. No new data is consolidated

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

3.4 Explain: Please elaborate as needed.
Not Applicable. The system FSS-19 does not monitor the public, GSA Employees, or contractors in any capacity

3.5 What kinds of report(s) can be produced on individuals?
Not Applicable. The system does not produce any reports on vendors

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?
Not Applicable. The system does not produce any reports on vendors

3.6 Why Not: Why will the data not be de-identified?
NA as data is not de-identified.

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?
Federal Agencies

4.2How: If so, how will GSA share the information?
Yes. Data is shared with other federal agencies via Inter Connections Agreement(ICD) documentation and or Memorandum of Understanding. (MOU)

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
The information is collected through the GSA SAM (System for Awards Management)

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?
For internal breach or suspected breach of PII, the process outlined in the applications IRP is executed. For breaches with external agencies, the process outlined in the MOA, ISA or MOU is executed.

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?
Accuracy and completeness of vendor information collected is handled by the registration module in sam.gov. Entity-entered TINs are validated by the IRS to ensure the TIN and Taxpayer Name provided matches the TIN and name control on file with the IRS. For completeness system validation rules ensuring required fields are populated correctly are in place. A record cannot be completed without all mandatory fields being completed

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

Application: FSS-19 PR Module
Role: FSSUser
Internal or External: Internal
Sensitivity Level: Moderate
Authorized Privileges and Functions Performed: Access to FSS-19 Database as a user.Access to Mainframe equates to default access to all databases with read access.FSSUser has only read access to FSS-19 databases

6.1b: What is the authorization process to gain access?
FSS-19 FSSUser Internal Moderate Access to FSS-19 Database as a user. Access to Mainframe equates to default access to all databases with read access. FSSUser has only read access to FSS-19 databases.

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.
8/22/2025

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The Eagan environment that houses the FSS-19 system has technical and physical security protections required for a FISMA Moderate system. The environment technical and physical and controls are detailed in the ClearPath SSP. The Technical controls that are documented in the FSS-19 SSP: - Identification and Authentication - Access Controls - Event auditing - Encryption at rest and transport - Vulnerability Scanning and Remediation The FSS-19 FISMA system has Managerial controls that are documented in the FSS-19 SSP and on the FSS-19 Google Team Drive. - Security Training - User access request procedures - Annual user recertification - Audit Review, Analysis, and Reporting - Security Assessments - Incident Reporting and Incident Response Plan

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?
The FSS19's System Owner and Information System Security Officer are responsible for oversight and management of the Application's security and privacy controls. All authorized users are responsible for immediately reporting any suspected loss, compromise, unauthorized access or disclosure of data from the system in accordance with the GSA rules of behavior and IT Security policies. The FSS19 Incident Response Plan outlines the steps and procedures to execute in the event any PII was lost, stolen or inappropriately accessed

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
FSS-19 Users are registered via Vendor registration process outside of FSS-19 as such the request to provide information is outside the scope of FSS-19 application

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
FSS-19 Users are registered via Vendor registration process outside of FSS-19 as such the request to provide information is outside the scope of FSS-19 application

7.2: What are the procedures that allow individuals to access their information?
FSS-19 Users are registered via Vendor registration process outside of FSS-19 as such the request to provide information is outside the scope of FSS-19 application

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?
The vendor cannot modify their information. The FSS 19 sub system is an internal application and does not offer amend functionality

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.
Individual (employees and contractors) with access to PII under the FSS-19 program have to complete the following training.

- "IT Security Awareness and Privacy Training 101" training within 30 days of employment.
- "IT Security Awareness and Privacy 101" training annually.
- Specialized Privacy Training 201 for managers/supervisors who work with PII as part of their duties.

GSA IT produces a report to identify individuals who have not taken the training and ensure the training is completed by everyone

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?
The System Owner along with the ISSO reviews and approves the responses documented against the controls related to PII in the Application's System Security Plan (SSP). The controls that align to the stated practices in this PIA and map the NIST PII controls are outlined under Chapter 13 of the FSS 19 System Security plan. 1. Access Control 2. Audit and Accountability 3. Identification and Authentication 4. Media Protection; Planning 5. Risk Assessment 6. System and Communications Protection; In addition the System Owner also ensures that controls in the SSP are validated by a third party who will audit the technical and policy safeguards, which include the PIA, ensure that information is used appropriately. FSS-19 implementation controls for PII is reviewed by the GSA Privacy assessment process and GSA Ongoing Authorization review program yearly.