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: 548
System Name: Federal Procurement Data System (FPDS)
CPO Approval Date: 9/14/2026
PIA Expiration Date: 9/13/2029

Information System Security Manager (ISSM) Approval

Arpan Patel

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Federal Procurement Data System (FPDS)

B: System, application, or project includes information about:
The FPDS is the government repository for information on government contracts and contains about 150 data elements per contract including but not limited to Taxpayer Identification Number (TIN) plus Contractor Names and

Addresses (for individuals contracting with the government as a business), Place of Performance and Socioeconomic Information about the Contractor.

C: For the categories listed above, how many records are there for each?
Currently, there are approximately 8 million of unique entities records in FPDS. Award: 76,047,488 IDV: 4,367,436

D: System, application, or project includes these data elements:
FPDS collects information about Contracts whose estimated value is $10,000 or more. Every modification to that contract, regardless of dollar value must be reported to FPDS. FPDS also maintains account data of government users, which includes:

- First name
- Last name
- Email
- Agency ID

The information above is captured during account registration. Government users are required to create account in order to submit data to FPDS. GSA's System of Record Notice (SORN) "GSA/OAP-3 Federal Procurement Data System" (FPDS)" applies to the information collected, maintained and disseminated.

Overview:

The Federal Procurement Data System (FPDS) is a centralized, mission-critical e-Government enterprise system managed by the General Services Administration (GSA). It operates as the single authoritative repository designed to optimize procurement logistics, lower operational overhead, and ingestion-stream real-time transactional contract data directly from distributed agency electronic commerce architectures. For compliance, oversight, and operational logistics, federal stakeholders and legislative bodies utilize FPDS reporting microservices to programmatically track small
business socioeconomic goals, audit cumulative contract volumes and obligation amounts, map geographical disbursement vectors, and compile vendor-specific performance portfolios.

The system's infrastructure is securely deployed inside a GSA-managed AWS Virtual Private Cloud (VPCaaS), operating as a certified component within the Federal Cloud Shared (FCS) multi-tenant resource environment. The deployment topology isolates workloads into three distinct cloud environments to safeguard system integrity. The FPDS Production instance handles
live, high-concurrency transactional database modifications from external agency procurement engines. This environment is supported by a mirrored FPDS Pre Production staging instance for pre-release validation and a decoupled Development and Test Facility (DTF) sandbox allocated for engineering, testing, and continuous integration pipelines.

Embedded within the primary ecosystem is the Interagency Contract Directory (ICD), a specialized sub-repository serving as an authoritative, public index for Indefinite Delivery Vehicles (IDV). Exposing its dataset via a dedicated frontend domain at contractdirectory.gov, the ICD allows procurement software and acquisition personnel to query, filter, and audit active intra-agency and interagency contract vehicles. This visibility enables contracting officers to

maximize existing vehicles and establish strategic procurement pathways prior to initializing new sourcing pipelines.

The application boundary relies on stringent access controls and modern identity federation. User authentication at the fpds.gov portal web frontend requires multi-factor authentication (MFA) brokered via an integration with the Login.gov identity provider interface.

At the data tier, the persistent storage engine—built on a PostgreSQL relational database architecture—implements granular database column-level encryption to mitigate data exfiltration vectors targeting sensitive acquisition metrics and Personally Identifiable Information (PII). Cryptographic lifecycle management is handled via an implementation of the IBM Security Guardium Application Encryption suite, leveraging a backend Thales CipherTrust Manager infrastructure. At the application layer, containerized microservices utilize a native JBOSS API to execute synchronous
cryptographic calls to the Thales CipherTrust Data Security Manager (DSM) server. This server stores the master symmetric keys, executes a strict 180-day automated key rotation policy to limit key cryptoperiod exposure, and enforces a high-entropy AES-256 cipher block chaining mode to ensure mathematical data protection across the data layer.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
For the Entity Management functional area of FPDS, 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). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

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?
GSA/OAP-3 Federal Procurement Data System ”Next Generation (FPDS-NG)"

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.
This series of records is concerned with creating and managing an information resource (e.g., Data.gov and USA.gov) for use or reference by the public and/or Federal agencies in carrying out their work. Included are change management decisions, planning documents, promotional materials, review reports, correspondence, and related records. Retention Instructions: Temporary. Cut off at the end of the fiscal year. Destroy 3 years after cutoff. Longer

retention is authorized if required to comply with requirements set forth in statutes, directives, agreements, contracts, OMB or GAO mandates, or similar authorities

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?
The SSN is stored within the FPDS database as a byproduct of the system receiving the SAM sensitive extract. FPDS does not populate contract actions with TIN (or SSN) data, and therefore does not disseminate the TIN/SSN within any outgoing data dissemination methods. The user does not enter TIN/SSN information within FPDS.

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?
In accordance with the Federal Information Security Management Act of 2002 (FISMA), every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. This PIA is included in the updated ATO package which will replace the package expiring on May 11, 2026. FISMA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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

3.4 Explain: Please elaborate as needed.
N/A

3.5 What kinds of report(s) can be produced on individuals?
Audit logs collected from the various resources and components supporting the FPDS production environment are reviewed and analyzed weekly by the appropriate technical team member. FPDS staff manually analyzes and correlate audit records across different repositories to gain situational awareness. They also integrate analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity. Permitted actions by each authorized information system process, role, and user are documented in the FPDS General Rules of Behavior and FPDS Role-based Rules of Behavior.

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?

The reports are designed to be publicly accessible and therefore do not contain information that requires aggregation or de-identification.

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?
No

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?
FPDS shares information from the Federal Procurement Data System (FPDS) with federal agencies through a combination of structured governance, secure connection methods, and automated data syndication.

Information sharing is legally restricted and managed via formal, bilateral Memorandums of Understanding and Interconnection Security Agreements (MOU/ISA). These documents are reviewed and approved by both partnering agencies, requiring final security sign-offs from the FPDS Information System Security Officer (ISSO) and Authorizing Official (AO) before any data pipeline is activated.

Depending on the specific architectural requirements of the consuming agency, GSA transmits the data via two primary channel types:

- Persistent Communication Channels: High-availability, dedicated connections such as T1 or T3 lines, Virtual Private Networks (VPNs), and Secure File Transfer Protocols (SFTP).
- Non-Persistent Communication Channels: Standard internet architectures, dedicated web portals, and secure Hypertext Transfer Protocol (HTTPS) endpoints.

GSA syndicates FPDS information downstream to external platforms and the broader public through two primary authoritative repositories:

- Interagency Contract Directory (ICD): Shared centrally via `contractdirectory.gov`, this text-based repository distributes Indefinite Delivery Vehicles (IDV) data to help contracting officers build intra-agency and interagency acquisition strategies.
- SAM.gov Data Bank: As part of GSA's ongoing modernization efforts, public search tools, standard reports, and web service data feeds are consolidated directly into the SAM.gov Data Bank, establishing it as the single authoritative portal for federal contract award data syndication.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Information is directly collected from the individuals wishing to extract data from FPDS-NG. Additionally a number of Agency Contract Writing Systems and Central Contractor Registration (CCR) send information to FPDS-NG. The CCR provides information to FPDS-NG on contractors doing business with the government.

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?
To enable the Federal Procurement Data System (FPDS) to interface with external systems or other internal General Services Administration (GSA) platforms, the participating entities must first establish a formal Memorandum of Understanding and Interconnection Security Agreement (MOU/ISA). This comprehensive framework undergoes a rigorous multi-agency review and approval cycle by all designated stakeholders before any technical integrations can commence. Within the GSA governance hierarchy, final authorization for the MOU/ISA is granted through official sign-offs from both the FPDS Information System Security Officer (ISSO) and the Authorizing Official (AO). Once the administrative and security guardrails are ratified, data transmissions are executed over either persistent communication channels, such as dedicated T1 or T3 lines, Virtual Private Networks (VPNs), and Secure File Transfer Protocols (SFTP), or non-persistent web channels including standard internet architectures, dedicated web portals, and secure Hypertext Transfer Protocol (HTTP) endpoints.

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?
Public users are verified through email. Agency users are verified through their email and agency admin.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Non-Privacy Act data is accessible to the public. Access to Privacy Act data is limited to authorized agency and contractor personnel (see list of agencies below):

- AGENCY FOR INTERNATIONAL DEVELOPMENT
- AGRICULTURE, DEPARTMENT OF
- AMERICAN BATTLE MONUMENTS COMMISSION
- BROADCASTING BOARD OF GOVERNORS
- COMMERCE, DEPARTMENT OF
- COMMODITY FUTURES TRADING COMMISSION
- CONSUMER PRODUCT SAFETY COMMISSION
- CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
- DEFENSE, DEPARTMENT OF
- EDUCATION, DEPARTMENT OF
- ENERGY, DEPARTMENT OF
- ENVIRONMENTAL PROTECTION AGENCY
- EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
- EXECUTIVE OFFICE OF THE PRESIDENT

- FEDERAL ELECTION COMMISSION
- FEDERAL EMERGENCY MANAGEMENT AGENCY
- FEDERAL ENERGY REGULATORY COMMISSION
- FEDERAL MARITIME COMMISSION
- FEDERAL TRADE COMMISSION
- GENERAL SERVICES ADMINISTRATION
- HEALTH AND HUMAN SERVICES, DEPARTMENT OF
- HOMELAND SECURITY, DEPARTMENT OF
- HOUSING AND URBAN DEVELOPMENT, DEPARTMENT OF
- INTERIOR, DEPARTMENT OF THE
- INTERNATIONAL TRADE COMMISSION
- J. F. KENNEDY CENTER FOR THE PERFORMING ARTS
- JUSTICE, DEPARTMENT OF
- LABOR, DEPARTMENT OF
- NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
- NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
- NATIONAL ENDOWMENT FOR THE ARTS
- NATIONAL ENDOWMENT FOR THE HUMANITIES
- NATIONAL GALLERY OF ART
- NATIONAL LABOR RELATIONS BOARD
- NATIONAL MEDIATION BOARD
- NATIONAL SCIENCE FOUNDATION
- NATIONAL TRANSPORTATION SAFETY BOARD
- NUCLEAR REGULATORY COMMISSION
- OFFICE OF PERSONNEL MANAGEMENT
- PEACE CORPS
- RAILROAD RETIREMENT BOARD
- SECURITIES AND EXCHANGE COMMISSION
- SMALL BUSINESS ADMINISTRATION

- SMITHSONIAN INSTITUTION
- SOCIAL SECURITY ADMINISTRATION
- STATE, DEPARTMENT OF
- TRANSPORTATION, DEPARTMENT OF
- TREASURY, DEPARTMENT OF THE
- UNITED STATES SOLDIERS AND AIRMENS HOME
- UNITED STATES TRADE AND DEVELOPMENT AGENCY
- VETERANS AFFAIRS, DEPARTMENT OF

6.1b: What is the authorization process to gain access?
The General Services Administration maintains a comprehensive Federal Procurement Data System (FPDS) System Security and Privacy Plan (SSPP) alongside an authoritative user guide to rigorously document system access controls and role-based permissions. Operational access within the environment is governed by the principle of least privilege, restricting user permissions strictly to the specific administrative or technical functions required by their organizational mandates. This granular role hierarchy includes distinct, predefined personas tailored to federal workflows, such as government procurement personnel executing acquisition actions and government debarment personnel managing vendor eligibility and compliance records.

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.
6/23/2029

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The Federal Procurement Data System (FPDS) enforces a defense-in-depth security posture structured across physical, technical, and managerial controls to safeguard federal contract data and maintain regulatory compliance.

Physical Security
The platform inherits FedRAMP High and DoD Impact Level physical protections by hosting within a GSA-owned AWS Virtual Private Cloud (VPCaaS) under Federal Cloud Shared (FCS) resources. AWS manages the physical perimeter using multi-layered access controls, biometric checkpoints, continuous video surveillance, and armed guards. Hardware maintenance is restricted to background-checked AWS infrastructure engineers.

Technical Security
The application boundary secures user ingress by requiring Multi-Factor Authentication (MFA) federated through Login.gov. Network topology isolates workloads into three decoupled environments including FPDS Production, Preproduction, and the Development and Test Facility (DTF). At the data layer, the PostgreSQL database implements granular column-level encryption for sensitive data and PII using IBM Security Guardium Application Encryption with Thales CipherTrust Manager. Containerized microservices use a native JBOSS API to execute cryptographic calls to a CipherTrust Data Security Manager (DSM) server, which enforces an AES-256 cipher and an automated 180-day key rotation policy. Inter-system data exchanges are restricted to persistent pipes (VPN, SFTP, T1/T3) or secure non-persistent web channels (HTTPS).

Managerial Security
System governance is dictated by an approved System Security and Privacy Plan (SSPP) and audited by the FPDS Information System Security Officer (ISSO) and Authorizing Official (AO). External integrations require a bilateral,

multi-agency approved Memorandum of Understanding and Interconnection Security Agreement (MOU/ISA). Internal operational access enforces the principle of least privilege through Role-Based Access Control (RBAC) defined in the FPDS user guide, segregating duties between specific personas such as government procurement personnel and government debarment personnel.

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?
he FPDS System Security Privacy Plan (SSPP), maintained under the system's Assessment and Authorization (A&A) boundary, dictates continuous monitoring via edge firewalls and specialized identity intrusion detection systems (IDS) calibrated to prevent PII exfiltration. For event orchestration, FPDS integrates directly with the GSA Enterprise Incident Response Plan (CIO-IT Security-01-02). This operational framework provides localized playbooks and standardized procedures for threat isolation, containment, and regulatory incident reporting.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Federal Acquisition Regulation (FAR) Part 4.1102(a) requires that: Offerors and quoters are required to be registered in SAM at the time an offer or quotation is submitted in order to comply with the annual representations and certifications requirements. The majority of the SAM registration data is Entity entered and Entity-certified via the following statement: I have read each of the FAR and DFARS provisions presented on this page. By submitting this certification, I, named company individual, am attesting to the accuracy of the representations and certifications contained herein, including the entire NAICS table. I understand that I may be subject to criminal prosecution under Section 1001, Title 18 of the United States Code or civil liability under the False Claims Act if I misrepresent named company in any of these representations or certifications to the Government. In short, anyone who wants to do business with the government must consent to registering in SAM. The Entity information in SAM is populated into FPDS at the time that a contract is awarded. FPDS reporting requirements are also directed by the Federal Acquisition Regulation (FAR); FAR 4.603 directs: (a) in accordance with the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. 109-282), all unclassified Federal award data must be publicly accessible, and (b) Executive agencies shall use FPDS to maintain publicly available information about all unclassified contract actions exceeding the micro-purchase threshold, and any modifications to those actions that change previously reported contract action report data, regardless of dollar value.

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.
To secure federal contract awards, vendors must complete a mandatory registration in the System for Award Management (SAM.gov). Upon contract award, the federal writing system programmatically pulls the validated vendor entity data from SAM.gov to populate the corresponding record within the Federal Procurement Data System (FPDS)

7.2: What are the procedures that allow individuals to access their information?
Individuals create the entity registration record in SAM.gov and can delete or amend the record. In addition, individuals can contact the system manager with questions about the operation of the Entity Management functional area. Requests from individuals to determine the specifics of an exclusion record included, should be addressed to the Federal agency POC identified in the exclusion record.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Once the user logs-into the FPDS portal, they have a feature to update or make edits to the individual user's information.

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.

The General Services Administration (GSA) mandates annual security awareness and privacy training for all personnel, enforcing strict governance policies regarding the proper handling of Personally Identifiable Information (PII). This curriculum explicitly outlines individual responsibilities for maintaining PII confidentiality and mitigating data exposure risk. Furthermore, to uphold the system security boundary, all Federal Procurement Data System (FPDS) operators granting access to PII are strictly required to undergo a favorable federal security background check and successfully clear a minimum of a Tier 1 background investigation.

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?

To ensure that information is handled strictly in accordance with the stated practices in the Privacy Impact Assessment (PIA), the Federal Procurement Data System (FPDS) system owner enforces a structured matrix of automated, operational, and administrative safeguards.

The application architecture enforces strict Role-Based Access Control (RBAC) brokered via Login.gov multi-factor authentication (MFA), programmatically restricting users to functions matching their authorized roles. Sensitive data and PII fields are isolated at the data tier using PostgreSQL column-level AES-256 encryption managed via IBM Security Guardium and Thales CipherTrust. Automated, unidirectional data ingestion from SAM.gov at contract award prevents manual manipulation of core entity records.

The system owner utilizes edge firewalls and identity intrusion detection systems (IDS) inside the GSA AWS Virtual Private Cloud (VPCaaS) to continuously monitor traffic. These systems track data access logs and flag anomalous behavior within the Assessment and Authorization (A&A) boundary. Any unauthorized data access attempt triggers immediate containment under the GSA Enterprise Incident Response Plan (CIO-IT Security-01-02).