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: 399
System Name: Federal Procurement Data System (FPDS)
CPO Approval Date: 12/2/2022
PIA Expiration Date: 12/1/2025

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Arda Odabasio

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-NG 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-NG. Award: 76,047,488 IDV: 4,367,436

D: System, application, or project includes these data elements:
FPDS-NG 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-NG. FPDS-NG also maintains account data of government and public, which includes: GOVERNMENT ACCOUNT:

- First name
- Last name
- Email
- Agency ID

PUBLIC ACCOUNTS (these data elements are considered PII):

- First name
- Last name
- Email
- Address
- City
- Country

The information above is captured during account registration. Government users are required to create account in order to submit data to FPDS-NG. Similarly, the public account users must also create an account in order to access publicly available data. GSA's System of Record Notice (SORN) "GSA/OAP-3 Federal Procurement Data System" ”Next Generation (FPDS-NG)" applies to the information collected, maintained and disseminated.

Overview:

The FPDS-NG is an e-Government initiative that has been developed to lower the government-wide cost of operations, be more responsive to the needs of its customers, and implement technology that enables data collection directly from agency electronic commerce systems. The Federal Procurement Data System – Next Generation (FPDS-NG) collects contract data from all agencies in the government. Congress and federal departments and agencies use FPDS-NG reporting capabilities to:

- Track small business goals
- Report number and amount of contracts to date
- Show geographical placement of contracts
- Summarize contract data for a specific contractor

FPDS-NG resides AWS Virtual Private Cloud owned by GSA consisting of;

- FPDS-NG Production.
- FPDS-NG Preproduction and DTF (Development and Test Facility)

Collectively, the above two instances are called FPDS-NG. IBM manages the technical aspects of FPDS-NG.

FPDS-NG includes the Interagency Contract Directory (ICD) which is a central repository of Indefinite Delivery Vehicles (IDV) awarded by the Federal agencies where the IDV is available for use at both the intra agency and interagency levels at contractdirectory.gov.

Small Business Dashboard smallbusiness.data.gov has been decommissioned and removed from the security boundary of FPDS per GSA direction in March 2019.

FPDS VPCaaS approved by GSA is not part of the BSP Mode 1,2 or 3 with no shared resources being used from mentioned BSP Modes.

MFA for fpds.gov frontend is currently implemented using login.gov. Postgresql database column encryption is currently not implemented, the IBM team and GSA team are actively planning and solutioning to implement these requirements with a tentative date by June 30, 2021.

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-NG, 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?
No

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA/GOVT-9 System for Award Management

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 (i.e. ATOM feeds or web services). 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 November 30, 2020. 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-NG 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?

Individual Agency Contract Writing Systems and the System for Award Management (SAM.gov) send information to FPDS-NG. The Contract Writing Systems send contract records directly to FPDS-NG through a secure SSL connection. SAM.gov provides information to FPDS-NG on Entities doing business with the government via a secure connection. eSRS, the subcontracting system, has access to FPDS-NG data through batch files. Electronic Subcontracting Reporting System (eSRS) receives contract actions via both a web service as well as an ATOM feed. eSRS requires data from FPDS in order to identify which contracts, as reported in FPDS, reach thresholds requiring a vendor to complete subcontract reporting for the given contract. eSRS is provided all contract actions, regardless of the 90 day delay on DoD funded actions. eSRS connections via web services are authenticated with a username/password. ATOM feed connections from eSRS are connected with a whitelisted IP address from the eSRS system that consumes FPDS data. All agencies and other organizations with access to FPDS-NG data through a secure connection must go through a documented certification process. The Certification Process Document is available on the FPDS-NG Project website at http://www.fpdsng.com under downloads.

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?
For FPDS to interact with other systems, either internally or externally to GSA there first must be a MOU/ISA established. The MOU is reviewed and approved by both partnering agencies. On the GSA side the ISA/MOU is approved by the Information System Security Officer (ISSO) and the Authorizing Official (AO) for FPDS. Data is transmitted either via a persistent pipe (TI, T3, VPN, SFTP, etc.) or a non-persistent pipe (internet, web portal, http, etc.)

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?
FPDS has a System Security Plan (SSP) as well as a user guide that documents access control and roles permissions. Roles are based on required function of the users, and include entities such as government procurement personnel and government debarment personnel.

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.
3/1/2019

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
FPDS Resides in the AWS within the GSA Business Service Platform (BSP) Platform as a Service (PaaS), ultimately leveraging the Amazon Web services US East (N.Virginia) Region.

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?

Monitoring activities are described in the FPDS-NG System Security Plan, which is part of the A&A. Which includes firewall protection, Identity intrusion detection; security controls are put in place to prevent the breaching of PII. In addition, FPDS utilizes GSA's enterprise Incident Response Plan (Incident Response (IR) CIO-IT Security-01-02) and has procedures in place for handling security incidents.

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-NG 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.
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-NG at the time that a contract is awarded.

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.
GSA requires privacy and security training for all personnel and has policies in place that govern the proper handling of PII. GSA employees receive annual security awareness training and are specifically instructed on their responsibility to protect the confidentiality of PII. All FPDS system users with access to PII are required to submit to a security background check and to obtain a minimum of a 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?

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, 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.