Federal Procurement Data System- New Generation (-NG)

Privacy Impact Assessment

March 21, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Stakeholders

Name & Email of Information System Security Manager (ISSM):

- Joseph Hoyt
- joseph.hoyt@gsa.gov

Name & Email of Program Manager/System Owner:

- Mary Searcy
- mary.searcy@gsa.gov

Signature Page

Signed:

_____

Information System Security Manager (ISSM)

_____

Program Manager/System Owner

_____

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for evaluating the PIAs for completeness of privacy related information.

Document Revision History

Date	Description	Version of Template
03/21/2019	Initial Draft of PIA Update	1.0

Table of contents

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about Federal Procurement Data System-Next Generation (-NG).The Integrated Award Environment (IAE) may, in the course of -NG, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.

System, Application or Project

Federal Procurement Data System New Generation (-NG)

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 toTaxpayer 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.

System, application or project includes

SECTION 1.0 PURPOSE OF COLLECTION

1.1 Why is GSA collecting the information?

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.

1.2 What legal authority and/or agreements allow GSA to collect 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).

1.3 **Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?**

The system does not have the capability to search using personal identifiers such as names or Social Security Numbers. Instead, users search the records by TIN, Contractor Name, Place of Performance and/or Socioeconomic Information about the Contractor to accomplish mission goals.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

System records are retained and disposed of according to GSA records maintenance and disposition schedules, the requirements of the Recovery Board, and the National Archives and Records Administration. For the Entity Management functional area, FPDS allows users to update and delete their own entity registration records. For the exclusions portion of the Performance Information functional area, electronic records of past exclusions are maintained permanently in the archive list for historical reference. Federal agencies reporting exclusion information in FPDS should follow their agency's guidance and policies for disposition of paper records.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

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.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

The primary privacy risk is that a data breach could result in the release of information on members of the public. This risk is mitigated by minimization of what is collected, limited access to the data, non- portability of the data, and controlled storage of the data in controlled facilities.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Yes, users are presented a privacy policy the bottom of the login screen that explains what information is collected and for what reason.
Like to the Policy: Security and Privacy

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

GSA has implemented various IT Security protocols and controls to secure the data in FPDS. Privacy risks are mitigated by controls designed to limit sharing of sensitive PII only by means of secure file transfer protocol (FTP) process through an Internet Protocol security (IPSEC) tunnel. GSA's SORN and FPDS-NG's privacy policy serve as openness and transparency measures.

SECTION 3.0 DATA MINIMIZATION

3.1 Whose information is included in the system, application or project?

Contractor and government and public account holder information is maintained within FPDS-NG.

3.2 What PII will the system, application or project
Contractor Taxpayer Identification Number (TIN), Social Security Number (SSN), plus Contractor Names and Addresses (for individuals contracting with the government as a business), Place of Performance, Product or service provided and Socioeconomic Information about the Contractor are maintained as are information for government and public account holders.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

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.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

There will be no new data created or derived based on the information collected.

3.5 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 March 14, 2018. 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. 3.6 Will the system monitor the public, GSA employees or contractors?

No, the system does not monitor the public. FPDS-NG employs firewalls, virtual private networks and security audit software that checks for attacks on the system as well as potential misuse or policy violations by users.

3.7 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 analyze 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

3.8 Will the data included in any report(s) be de-identified? If so, what process (es) will be used to aggregate or de-identify the data?

No. The reports are designed to be publicly accessible and therefore do not contain information that requires aggregation or de-identification.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

There are no identifiable risks associated with data minimization for
FPDS-NG because system has been designed to maintain the minimum amount of information necessary to accomplish the business and mission goals

SECTION 4.0 LIMITS ON USES AND SHARING OF 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?

Please reference the answer for #2 above. FPDS does not collect or display the SSN on a contract action, and therefore does not disseminate this data through any outbound data dissemination methods.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? 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. 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 or is it taken from another source? If so, 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? If so, who, how and is a formal agreement(s) in place?

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.)

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Potential risks related to data sharing and use limitation are addressed during the MOU/ISA development process between GSA and partnering agencies.

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

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

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

There are no identifiable risks associated with data quality and integrity for this system.

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

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

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 GSA completed a system security plan for the information system(s) or application?

Yes, in March 2019. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). FPDS is conducted on systems rated "moderate impact." Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" to secure its systems and data.

6.3 How will the system or application be secured from a physical, technological, 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 suspected or confirmed security incidents and breaches of PII? If so, what are they?

Monitoring activities are described in the FPDS-NG System Security Plan, which is part of the C&A. Which includes firewall protection, Identity intrusion detection; security controls are put in place to prevent the breaching of PII.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

Yes, the potential risk of unauthorized use or disclosure of PII is always present. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans. In addition, access is limited on a need to know basis, with logical controls limiting access to data.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

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.

7.2 What procedures 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? If so, how?

Yes, individuals can contact the system manager with questions about the operation of the Entity Management functional area.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Yes. Regardless of whether individuals choose to participate or not, GSA may create administrative-trace data acknowledging their choice. This information describes, at minimum, a potential relationship between an individual and GSA. GSA has assessed and approved access controls to administrative data; GSA promotes transparency and encourages public feedback through this PIA, and through public comments to Information Collection Requests and SORNs published in the Federal Register.

SECTION 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.

8.2 Are there any privacy risks for this system, application or project that relates to awareness and training? If so, how will GSA mitigate these risks?

GSA's privacy and security awareness and training programs are designed to address questions about PII and how to handle it at the enterprise level, thereby covering potential risks related specifically to FPDS.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system, application or project ensure that the information is used in accordance with 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes. In keeping with NIST 800-53 rev 4, control number AR-4, GSA regularly assesses its programs to ensure effective implementation of privacy controls. While some of these assessments can be automated, such as those carried out via GSA's CloudLock tool, others are carried out via GSA or third party auditors.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA's Privacy Office.