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: 328
System Name: System for Award Management (SAM)
CPO Approval Date: 7/15/2020
PIA Expiration Date: 5/2/2024

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Robert Donovan

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
System for Award Management (SAM)

B: System, application, or project includes information about:
SAM is the trusted, essential place to seamlessly connect to the business of government. As such, Beta SAM collects information on entities registering to do business with the U.S. government in accordance with Federal Acquisition

Regulation (FAR) Subpart 4.11 and Title 2 of the Code of Federal Regulations (2 CFR) Subtitle A, Chapter I, and Part 25. Part of the registration data collected from entities which pay U.S. taxes is the Taxpayer Identification Number (TIN). The TIN is usually the entity's Employer Identification Number (EIN). However, sole proprietors and single-member limited liability companies can elect to use their Social Security Number (SSN) as their TIN. The system also collects as part of registration process, names of (First, Last and Middle) individuals registering as Sole Proprietorship and addresses of entities and individuals registering to do business with the U.S Government.

C: For the categories listed above, how many records are there for each?
About 1.4 million record estimated for all the categories listed above

D: System, application, or project includes these data elements:
Beta SAM provides detailed, public descriptions of federal assistance listings available to State and local governments (including the District of Columbia); federally recognized Indian tribal governments, Territories (and possessions) of the United States; domestic public, quasi- public, and private profit and nonprofit organizations and institutions; specialized groups, and individuals. There are different types of award data, or "domains". A user will be able to search across all domains or choose a specific domain to search within a specific data set. The table below provides a view of detailed records for all domains: Domain Description Assistance Listings Find assistance listings by entering a keyword, Catalog of Federal Domestic Assistance (CFDA) number, or agency name into the search field. Contract Opportunities Find contract opportunities by entering a keyword, solicitation ID, or an agency name into the search field. Contract Awards Find contract award data by entering a keyword, award type, North American Industry Classification System (NAICS) Code, Product Service Code (PSC), or DUNS ("data universal numbering system"). Entity Registrations Find entity registrations by entering an entity's name into the search field. The search filter will automatically display "active" entities, but you can also switch to view only inactive results. Entity Exclusions Find exclusions associated with a particular entity by entering the entity's name, DUNS number, or Commercial and Government Entity (CAGE) code. To search for a person, type in his or her name. Be sure to confirm that you've found the correct person ”it's easy to misidentify someone if he or she has a common name. If no exclusion record is found for the entity, the entity does not have an active exclusion in SAM. Federal Hierarchy Enter a department or sub-tier. Use the Federal Hierarchy filter to narrow your results. Wage Determinations Contract Data Report Find applicable Service Contract Act (SCA) and Davis-Bacon Act (DBA) wage determinations required for each contract action by entering a wage determination (WD) number or using the filters to narrow down your results by geographic location. Find and run standard, static, administrative, and ad hoc contract data reports. Users may use the reports to search public award data to find competitive information and build their business pipelines. Users can learn when existing contracts expire and to help identify potential subcontracting opportunities. Federal agencies use this data to measure, analyze, and report on how federal contracting affects the U.S. economy and the success of policy.

Overview:

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 SAM, 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/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.
System records are retained and disposed in accordance with 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, Beta.SAM 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 Beta.SAM follows the agency's guidance and policies for disposition of paper records.

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.
For the Entity Management functional area, individuals are aware that SAM contains a record on them because they created the record through a self-registration portal. For the exclusions portion of the Performance Management functional area, individuals receive prior notification of their exclusion from Federal procurement and non-procurement programs

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
SAM collects necessary information from individuals and entities seeking to do business with the U.S Government. The information is required to create a profile/record for the entity/individuals, establish and validate the applicant's identity, determining the eligibility of various awards/grants/programs/benefits and in furtherance of the Beta SAM mission and business processes. The exclusion records on individuals contain information that is not publicly displayed (e.g., street address information, as well as the SSN or TIN). Agencies disclose the SSN of an individual to verify the identity of an individual, only if permitted under the Privacy Act of 1974 and, if appropriate, the Computer Matching and Privacy Protection Act of 1988, as codified in 5 U.S.C. 552(a).

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 Modernization Act of 2016 (FISMA), all GSA system must receive a signed Authority to Operate (ATO) from a designated GSA 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 to maintain the security posture of the information system. FISMA controls implemented contains 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. The following specific controls are implemented to protect the confidentiality, integrity and availability of the Beta Sam system and the data transmitted, processed, and stored within the environment of operation:

Management Controls

- Certification, Accreditation and Security Assessments (CA)

- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational Controls

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA) Media Protection (MP)
- Physical and Environment Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical Controls

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Privacy Controls

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

Additionally, all GSA employees are required to take annual security awareness training, which addresses privacy and handling of PII data. GSA also maintains rules of behavior for employees who use GSA systems and limits access to PII by employing role-based access (only allowing access to users who need PII to perform their duties.

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

3.4 Explain: Please elaborate as needed.
No, SAM system is not designed to monitor the public, GSA employees or contractor. However, SAM resides in a Container-as-a-Service (CaaS) Cloud environment. There are various monitoring tools configured to monitor, and log/audit the system applications to enhance the incident management capabilities.

3.5 What kinds of report(s) can be produced on individuals?
SAM does not produce any reports on individuals. All reports are pertaining to contracts (contract data reports), grants, or FAR requirements. In the event of a sole proprietor, the report will be pertaining to contracts, grants, or FAR requirements but may contain PII, if PII is used in the sole proprietor's business operations.

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?
This will need to updated in 2022

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?
Federal agency Contract Writing Systems (CWS), grants management systems, and financial systems will all use data from Beta.SAM. They go through a data access request process to allow them certain levels of data. The data is provided over encrypted connections and are either SFTP or web services (XML) and managed through role management. Part of the access process includes a Non-Disclosure Agreement and System Authorization Access Request (System Account) which is agreed to by the requestor during the data access request process and includes user responsibility regarding the data. Also, users (Federal and Non-Federal) may access beta SAM data using a system account. Federal and Non-Federal users must submit a System Account Application to request access to Beta SAM. The application is reviewed for business justification, need to know, valid authorization and other security requirements. Once approved users are granted access to Beta.SAM.gov APIs. The application process is through an automated self-service portal on Beta.Sam.gov to request a system account

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Entity records are created by the person or entity wishing to do business with the government. Exclusion records are created by Federal agency suspension and debarment personnel.

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?

SAM may interact with other systems either internally or externally to GSA there must be an MOU/ISA established for such interaction. The MOU/ISA is reviewed and approved by both partnering agencies. On the GSA side, the SAM MOU/ISA is approved by the ISSO and the Authorizing Official (AO) for SAM. 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?
To verify accuracy, system validation rules exist. 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. Access to edit an entity record is controlled through roles and permissions. 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?
SAM has a System Security Plan (SSP) as well as a user guide that thoroughly documents access control, roles, and permissions. Access to data in the system, application, or project is restricted to authorized user only commensurable to their approved role and permission. Roles are based on the required function of the users, and include the entities, government procurement personnel, government debarment personnel etc.

6.1b: What is the authorization process to gain access?
Access to data in the system, application, or project is restricted to authorized user only commensurable to their approved role and permission. Roles are based on the required function of the users, and include the entities, government procurement personnel, government debarment personnel etc.

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.
5/21/2021

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
SAM resides in the GSA FAS Cloud Services (FCS) Platform as a Service (PaaS)/Container as a Service (CaaS) Mode 3 model, ultimately leveraging the Amazon Web Services (AWS) East/West Region. Also, the information system has implemented technical, operational, management and privacy control to secure the system and its data and maintain the security posture of the system.

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?
SAM resides in the AWS Cloud environment (Container as a Service) with various automated mechanism in place for logging/auditing using Cloud Watch, Slunk, and application monitoring (New Relic) for incident management in accordance with the GSA policies and procedures for handling security incidents. Responsible system and technical officers report any potential incidents directly to the relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Individuals do not have opportunities to opt out or decline to provide information to Beta.SAM. Most of the data collected by the system is related to agency entities which are provided by a company pursuant to applicable laws and regulations rather than directly from users. Additionally, data collected by Beta.SAM entities is related to their access and use of the system and is collected through use of the system

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.
Individuals do not have opportunities to opt out or decline to provide information to Beta.SAM. Most of the data collected by the system is related to agency entities which are provided by a company pursuant to applicable laws and regulations rather than directly from users. Additionally, data collected by Beta.SAM entities is related to their access and use of the system and is collected through use of the system

7.2: What are the procedures that allow individuals to access their information?
Since individuals/entities created the entity registration record in Beta.SAM through a self-registration portal, there are no restriction or limitation to managing such data. Users can delete, update, or amend the record at will. However, 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 in Beta.SAM 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?
Yes, since individuals create the entity registration record in Beta.SAM through a self-registration portal, there are no restriction or limitation to managing such data. Users can delete, update, or amend the record at will. However, 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 in Beta.SAM should be addressed to the Federal agency POC identified in the exclusion record.

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 governs 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 SAM 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, Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. GSA takes automated precautions against overly open access controls. GSA's CloudLock tool searches all GSA documents stored on the Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.