System for Award Management (SAM)

Privacy Impact Assessment (PIA)

July 16, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

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

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Joseph Hoyt

Name of Program Manager/System Owner:

- Calvin Densmore

Signature Page

Signed:

DocuSigned by:
Joseph Hoyt
CA8EF810EDA7425...

Information System Security Manager (ISSM)

DocuSigned by:
Calvin Densmore
5BBDED15A27A471...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183E40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

Table of contents

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 (SSP) for the information system(s) supporting the project?

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

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about System for Award Management (SAM). To accomplish its mission *GSA* Integrated Award Enterprise (IAE) must, in the course of SAM, 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]

A. System, Application, or Project Name:

System for Award management (SAM)

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

The 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.

C. For the categories listed above, how many records are there for each?

Currently, there are approximately 5.6 million of unique entities records in SAM.

- Entity Management Records (Registered Entities): 2331615
- Shell Records (Non-Registered Entities): 3063921
- Exclusions: Count :203021

D. System, application, or project includes these data elements:

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

Overview

The Integrated Award Environment (IAE) is a Presidential E-Gov initiative. Its purpose is to simplify, unify and streamline the complex federal award process for government buyers and sellers. There are acquisition functions common to all agencies that are now centrally managed as shared systems. This is accomplished through reuse, sharing data, linking systems and making data accessible to all.
SAM.gov stores entity information for those wishing to do business with the Federal Government. Entities are required to update their information anually as mandated by regulation. Entities have the responsibility to maintain their own information to assist contracting and grant-making officials in their pre-award determinations and management of the federal awards throughout the lifecycle.
The following PII are collected during registration:

- 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
- Legal Business Name and Physical Address.
- Bank's routing number, bank account number, and bank account type.

SECTION 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).

1.3 Has an 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, 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 SAM should follow their agency's guidance and policies for disposition of paper records.

1.4 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.

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, 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 SAM should follow their agency's guidance and policies for disposition of paper records.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes users are presented a Privacy Policy at the bottom of the login screen that explains what information is being collected and for what reason.

Link to the Policy: https://sam.gov/SAM/pages/public/generalInfo/samPrivacyPolicy.jsf

For the Entity Management functional area, individuals know that SAM contains a record on them because they created the record. For the exclusions portion of the Performance Management functional area, individuals receive prior notification that their names will be contained in SAM from the Federal agency that takes the action to exclude them from Federal procurement and non-procurement programs.

SECTION 3.0 DATA MINIMIZATION

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

Exclusion records on individuals contain certain information that will never be displayed publicly, 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? If so, how will this data be maintained and used?

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

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 replaced 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.

3.4 Will the system monitor the public, GSA employees, or contractors?

No, there is no monitoring capability in SAM.

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, 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? If so, what process(es) will be used to aggregate or de-identify the data?

No, it will not be used to aggregate or de-identify

SECTION 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?

SAM maintains this Government wide system of records to enable Federal agencies to determine who is registered to do business with the Federal Government, and to identify individuals who have been excluded from participating in Federal procurement and non-procurement (financial or non-financial assistance and benefits programs), throughout the Federal Government. In some instances a record may demonstrate an exclusion applies only to the agency taking the action, and therefore does not have Government wide effect. The purpose of the exclusions is to protect the Government from non-responsible contractors and individuals, ensure proper management throughout the Federal government, and protect the integrity of Federal activities.

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?

Yes. Federal agency Contract Writing Systems (CWS), grants management systems, and financial systems will all use data from 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 FTP or web services (XML). Part of the access process includes a Non-Disclosure Agreement and System Authorization Access Request which is agreed to by the requestor during the data access request process and includes user responsibility regarding the data.

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)?

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? If so, who and how? Is a formal agreement(s) in place?

For SAM 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 SAM. Data is transmitted either via a persistent pipe (TI, T3, VPN, SFTP, etc.) or a non-persistent pipe (internet, web portal, http, etc.)

SECTION 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 though 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.

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?

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

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes, in December 17, 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). Sam is conducted on systems rated "moderate impact." Based on this categorization, GSA implements security controls from 15 Version 1.0: March 27, 2019

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, technical, and managerial perspective?

SAM 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? If so, what are they?

SAM.gov utilizes GSA's enterprise Incident Response Plan (Incident Response (IR) CIO-IT Security-01-02) and has procedures in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any potential incidents directly to the Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? 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 SAM. Most of the data collected by the system is related to entities which are provided by a company pursuant to applicable laws and regulations rather than directly from users. Additionally, data collected by SAM entities is related to their access and use of the system and is collected through use of the system

7.2 What procedures allow individuals to access their information?

Since individuals create the entity registration record in SAM and can delete or amend the record, there should not be any questions about that entry. 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 SAM 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.

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 governs the proper handling of PII. 17 Versions 1.0: March 27, 2019

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.

SECTION 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.

---

[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.