System for Award Management (SAM)

Privacy Impact Assessment

May 30, 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:

- Marci Eaton
- marci.eaton@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
03/20/2018	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 the System for Award Management (SAM). . 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

SAM.gov

SAM.gov is a governmentwide repository of 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.

A required data field s is the Taxpayer Identification Number (TIN).

Key data sets in SAM.gov include:

Search Criteria	**Description**
	.
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 Why is GSA collecting the information?

GSA has established a system of records subject to the Privacy Act of 1974 (as amended), 5 U.S.C. 552a.

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

Records are retrievable by searching against information in the record, including, but not limited to, the person's or entity's name, DUNS number, SSN and TIN. However, searching for registration records by TIN is limited to Federal Government users and searching for exclusion records by SSN or TIN requires an exact name match as well.

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, 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.

1.5. 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.

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.

1.6. 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 to members of the public. This is mitigated by limited access to the data, non- portability of the data, and controlled storage of the data in controlled facilities. In addition, GSA trains its employees to identify potential incidents and report them immediately, providing incident response early notice to remediate potential harm.

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 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.

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

Privacy risks are mitigated by ensuring that the sharing of sensitive PII is only performed by means of secure file transfer protocol (FTP) process through an Internet Protocol security (IPSEC) tunnel.

SECTION 3.0 DATA MINIMIZATION

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

The system collects, maintains and uses information about contractors/vendors, Federal and non-federal employees, and anyone 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.

3.2 What PII will the system, application or project include?

In the Entity Management functional area, SAM contains records that capture information users voluntarily provide about their entity as part of the process to register to do business with the Federal Government, including the entity legal business name, entity email address, entity telephone number, entity Taxpayer Identification Number (TIN), and entity address.

In the case of a sole proprietor, tax laws allow them to use their Social Security Number (SSN) as their TIN if they do not have a separate Employer Identification Number (EIN). The TIN (whether it be an EIN or an SSN) is not publicly available data. In the exclusion portion of the Performance Information functional area, SAM contains records entered by Federal agency suspension and debarment officials, some of which may be records on individuals.

3.3 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).

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

No new data will be 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 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.

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

No, there is no monitoring capability in SAM.

3.7 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.

3.8 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

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 SAM. GSA has reviewed

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?

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, how and 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.)

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?

There are no risks associated with use limitation for this system. 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?

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.

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?

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 for the information system(s) or application?

Yes, in November 2017. 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

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?

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 suspected or confirmed security incidents and breaches of PII? If so, what are they?

GSA 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 relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

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?

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. GSA also automates protections against overly open access controls. For example, GSA's CloudLock tool searches all GSA documents stored in 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.

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.

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.

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 a minimum, a potential relationship between an individual and GSA. Modernized SAM.gov PIA GSA mitigates this risk through appropriate access controls to administrative data; GSA promotes transparency and encourages public feedback through this PIA, and through public comments to Information Collection Requests 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 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.

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

There are no risks associated with awareness and training for this system.

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, 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.

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 its Sam and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA's Privacy Office.
