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: 497
System Name: Assisted Services Shared Information System (ASSIST)
CPO Approval Date: 5/19/2025
PIA Expiration Date: 5/18/2028

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Assisted Services Shared Information System (ASSIST)

B: System, application, or project includes information about:
The ASSIST system collects information on entities registering to do business with the U.S. government allowing GSA to create an order for a client; solicit bids from contractors capable of fulfilling the order (or submit a direct buy to a specific contractor); assign funding to the order; and finally award the order to a winning bidder. ASSIST also

includes information allowing for client and contractor registration, order modification, order accrual generation, invoice tracking, output file generation for GSA Finance, vendor performance reporting, client satisfaction reporting and file attachments for documentation purposes on the majority of the documents within the system.

C: For the categories listed above, how many records are there for each?
About 2.6 million records are estimated for all the categories listed above.

D: System, application, or project includes these data elements:
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 singlemember limited liability companies can elect to use their Social Security Number (SSN) as their TIN. The system also collects email addresses and 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.

Overview:

ASSIST is an online integrated purchase order fulfillment and client/vendor relationship management system. The basic workflow within the system allows for GSA to create an order for a client; solicit bids from contractors capable of fulfilling the order (or submit a direct buy to a specific contractor); assign funding to the order; and finally award the order to a winning bidder. Additional functionality allows for client and contractor registration, order modification, order accrual generation, invoice tracking, output file generation for GSA Finance, vendor performance reporting, client satisfaction reporting and file attachments for documentation purposes on the majority of the documents within the system.
ASSIST provides mission critical business processes and financial functions to support the GSA FAS Assisted Acquisition Services (AAS) business line. Additionally, ASSIST is a multi-tenant, shared service platform that provides other business line consumers and organizations segmented business processes and financial support. ASSIST is currently composed of a combination of ASSIST2 and legacy components (supporting registration, and shared, consolidated processes under the ASSIST 1.0 platform). For GSA's assisted-acquisition community, their clients and contractors who want to manage all facets of assisted acquisition in an automated fashion, the ASSIST platform is a centralized series of consumable services that eliminates other duplicative systems.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
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.

The records retentions schedule is in accordance with GSA and GRS Records Retention Schedules | 1.0 - Finance, GRS 01.1/010 Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. DAA-GRS-2013-0003-0001 (https://insite.gsa.gov/system/files/insite/GSA_Records_Retention_Schedule_4_10_2020.pdf) Electronic records of past exclusions are maintained permanently in the archive list for historical reference. Federal agencies reporting exclusion information in 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.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
ASSIST 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 ASSIST and 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 systems 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 ASSIST 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
○ PII Processing and Transparency (PT)
○ Program Management (PM)
○ Supply Chain Risk Management (SR)
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, the ASSIST system is not designed to monitor the public, GSA employees or contractor. However, ASSIST exchanges information with SAM.gov which 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?
ASSIST 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?
Data considered as sensitive provided in reports are not de-identified because such data are provided on request by authorized parties who have a need to know and are authorized to view the data. All Data considered as Public data can be viewed by the public. To search data in ASSIST, users must authenticate to GSA systems using multifactor authentication prior to granting access.

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 ASSIST. 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 NonDisclosure 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 ASSIST data using a user account within ASSIST based on Role-based requirements. Federal and Non-Federal users must complete registration on ASSIST before access to ASSIST is granted. The registration process is provided through an automated self-service portal on the ASSIST website.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

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?
ASSIST interacts with other systems either internally or externally. Data is transmitted securely over either a persistent pipe (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, individuals can access their own personal data in the registration area of the ASSIST system and edit the following information: email, Business Phone Number, Business Address. Individuals can also ask GSA to correct records that are inaccurate, incomplete, untimely, or irrelevant. See https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-of-1974 for more information.
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?
Users will have access to information that they provide in the system and applications while interacting with the system. Additionally, ASSIST identifies user authorizations for access to data in systems and applications based on the roles and the required functions of the users, and include the entities, government procurement personnel, government debarment personnel etc. The user access controls are documented in the ASSIST System Security and Privacy Plan (SSPP).

6.1b: What is the authorization process to gain access?
Access to data in the system, application, or project is restricted to authorized users 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. Note that all user access is through a Role-Based Access Control and users are required to authenticate through using GSA-approved multifactor authentication prior to accessing the information system.

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.
7/7/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
ASSIST operates as a tenant of the GSA FAS Cloud Services (FCS) leveraging the Amazon Web Services (AWS). ASSIST also leverages services of ServiceNow and NICE CXone FedRAMP provisionally authorized Software as a Service (SaaS) systems. Also, the ASSIST 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?
ASSIST resides in an AWS Cloud environment with various automated mechanisms in place for logging/auditing for incident management in accordance with the GSA policies and procedures for handling security incidents. ASSIST also leverages services of ServiceNow and NICE CXone FedRAMP provisionally authorized Software as a Service (SaaS) systems which support FedRAMP requirements for mechanisms to identify and respond to suspected or confirmed security incidents and breaches of PII. 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 ASSIST.

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 ASSIST in order to maintain transactional integrity and traceability.
Data collected by the system relates to mission critical business processes and financial functions to support the GSA FAS Assisted Acquisition Services (AAS) business line and for providing other business line consumers and organizations segmented business processes and financial support. Additionally, client and contractor registration, order modification, order accrual generation, invoice tracking, output file generation for GSA Finance, vendor performance reporting, client satisfaction reporting and file attachments for documentation purposes on the majority of the documents within the system.
Services provided to individuals and agency entities pursuant to applicable laws and regulations rather than directly from users. Additionally, business data is collected by ASSIST entities and relates to an individuals' 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?
Individuals create and update through the ASSIST portal using the procedures and guidance provided for the ASSIST services. Individuals can ask GSA for access to records about themselves in accordance with the GSA's Privacy Act Rules. However, when a system is exempt from certain sections of the Privacy Act, there may be limitations on the disclosure or amendment of records. See: https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-of-1974

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?

Individuals can request amendment for information about themselves through the ASSIST portal. There are no restrictions or limitations to managing such data. Individuals can request updates or amendments to records as needed for business purposes. Requests from individuals to amend information are addressed through the ASSIST portal.

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 ASSIST 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 employs security tools to protect all GSA documents stored on the Google Drive to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.