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: 541
System Name: Personal Property Management System (PPMS)
CPO Approval Date: 6/24/2026
PIA Expiration Date: 6/23/2029

Information System Security Manager (ISSM) Approval

Anthony Konkwo

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Personal Property Management System (PPMS)

B: System, application, or project includes information about:
Personal Property Management System modernization

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

300 Internal GSA users, 10,000 federal and state users and approximately 100,000 general public, public company, schools and other organizational users

D: System, application, or project includes these data elements:
General Public:
Name and date of birth
Contact Information (addresses, telephone numbers, and email address)
Social Security Number
Financial Information (credit card numbers and expiration dates)
Information about individuals provided by third parties (accept or refer decision from Experian PreciseID identity proofing service)

Public Companies:
Representative Name
Business name
Contact Information (addresses, telephone numbers, and email address)
TIN
Information about Company provided by third parties (accept or refer decision from Experian BizId identity proofing service)

Schools / Universities:
Representative Name
School Information
Contact Information (addresses, telephone numbers, and email address)
Government-issued Organization identifiers

Federal and State Users:
Name
Agency Information
Contact Information (addresses, telephone numbers, and email address)

Overview:

The Personal Property Management Systems Modernization Project replaces disparate legacy Personal Property Management (PPM) IT Systems (GSAXcess, SASy, GSA Auctions, MySales, Computers For Learning (CFL), AAMS and Foreign Gifts and GovSales) with a modern solution that enables GSA to effectively fulfill its mission in personal property disposal. It also enables FAS/GSS to reduce full time equivalent (FTE) direct labor and IT support costs, enhance the range and level of services that PPM can offer to Federal customers, and improve operational efficiency.
The modernization of this system is currently in production.

The capabilities of the system under development include:

- Receive and track property data.
- Publish information to an online marketplace, where transaction options include federal transfer (reutilization), donation, public auction, or removing unsold/donated/auctioned items from the marketplace (i.e., returning the item back to agency)
- Maximize bidder participation and sales proceeds.
- Move unneeded property out of Federal Government control as quickly as possible - reducing holding costs.
- Maintain data including historical sales trends to optimize screening times and improve decision making.
- Automate low value and resource intensive processes.
- Reduce days to reimburse customers for sales proceeds.

To better understand the scale and financial impact of this system, during fiscal year 2018, the Office of Personal Property Management:

- Facilitated the reutilization of $1.14 Billion of personal property within the government
- Donated $397 Million of personal property to state and local governments and other
- eligible non-Federal recipients
- Sold $173.7 Million in personal property to the general public, of which $142.4 Million
- was returned to Federal agencies

The modernized Personal Property Management System (PPMS) is developed using microservices architecture to be in alignment with GSA IT's modernization approach and replaces the existing 7 legacy systems into one consolidated system. Figure 1 below depicts the core components of the PPMS architecture.

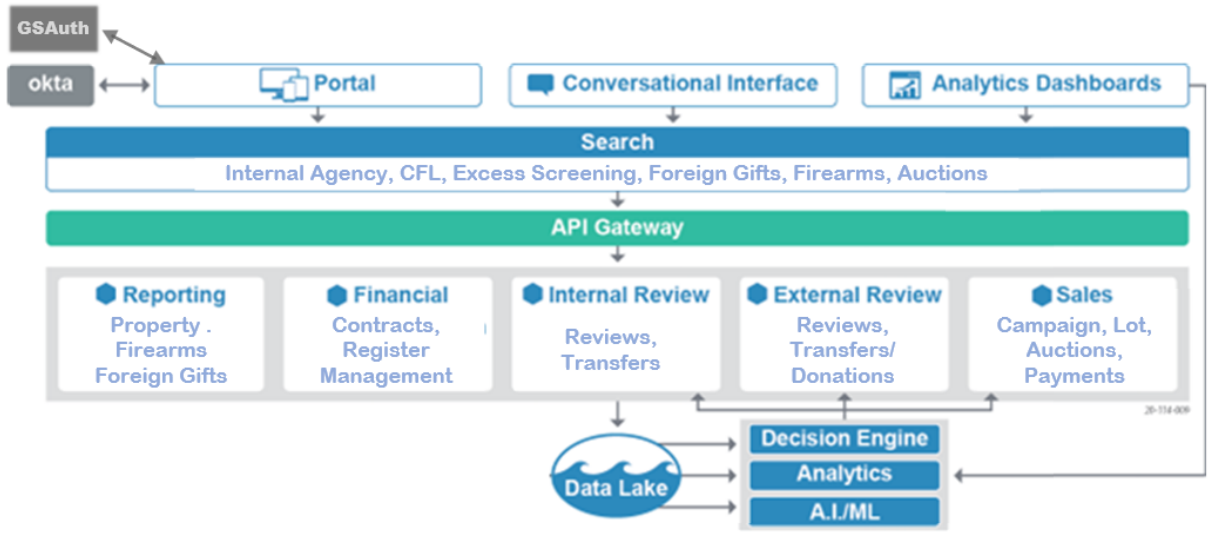

Figure 1: Technical services aligned to Business architecture for PPMS

A new data model is created for the modernized system and existing data is migrated into the new data model. The new PPMS system leverages FCS cloud to maximize use of common security control and services and its VPCaaS for use of a microservices architecture and CI/CD services not currently available in the FCS. The modernized system integrates with external systems/interfaces such as GEIP, GSAuth, Pay.gov etc. to support the business functions. In addition, it will also align to GSA IT system architecture & UI interface. Authentication is implemented using SAML with GSAuth to support single sign on for internal users and GEIP for external users. Figure 2 below depicts the primary functions performed by the components of the PPMS architecture.

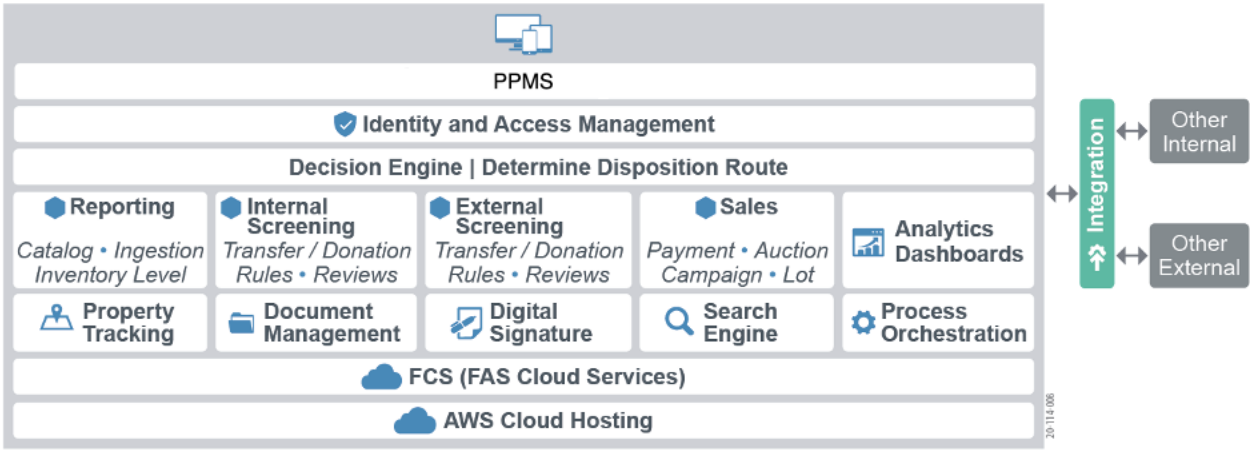

Figure 2: Functional Architecture of PPMS

The modernized system will handle large volumes of data and multiple concurrent users accessing the system. Users for the system include Federal Agency users, State agency users, General public, small businesses and international users.

Table 9.0-1. Estimated Required Capacity for PPMS System

Average Concurrent Users	2500
Surge Concurrent Users	15000 Note: Some modules can have higher concurrent users with occasional situational surge (high demand featured auctions)

Application Architecture

PPMS functionality requires Property Reporting, Property Reuse/Sales, Payment, Financial Management, Inventory, Management, Marketing, Portals, Service Interface, Identity & Access management, Data Migration/Management, General Requirements and Workflow.

In alignment with GSA's IT modernization approaches, we propose a microservices architecture that allows re-use and delivers these business services and capabilities. Employing Domain-Driven Design (DDD), we decompose the existing monolithic system into a suite of independently deployable modular and loosely coupled microservices. Each service operates and manages a unique process and communicates through a well-defined, lightweight mechanism to accomplish a business goal. The services are small, independent, self-contained, independently deployable, and scalable. They are highly decoupled and focus on a small task or capability following the Single Responsibility Principle. The only dependency these code bases have on one another is their Application Programming Interfaces (APIs), that make future changes/enhancements easy. Team REI will utilize open source platform Spring Boot and Aurora to install, configure, and customize business services rapidly.

Presentation Layer

The Presentation Layer is developed with SPA architecture. This presentation layer is

developed using client side MVC/SPA framework (React) rich user interface that will adapt to different screen sizes (Bootstrap). The Presentation Layer will communicate with the PPMS API microservices layer through representational state transfer application programming interface (RESTful API) Web service calls.

Application Services

Application layer is developed using the Java Spring Boot technologies and is exposed with REST Services to the presentation layer. Open API specification is used to document and publish the APIs.

Data Layer

The data tier will provide storage for records and files. It will leverage native and PaaS capabilities of FAS cloud, specifically RedShift and Tableau. AWS RDS MySQL is used for standard database record storage for the PPMS System, and RDS Postgres is used by the CI/CD Pipeline by SonarQube. Customer Address File (CAF) Services are data services that provide customer organization and address information to GSA IT systems from the FSS-19 CAF Database. The objective of this interface is to support the Federal Acquisition Regulation (FAR) change to verify that systems use an Activity Address Code (AAC) that exists in the Department of Defense Activity Address Directory (DoDAAD).

PCI Layer

Credit card information stored and used in the system for payments conforms to PCI-DSS standard. At rest encryption of PCI data is performed using AWS RDS configurations, in addition to column level encryption of the specific PCI data fields managed by the PPMS application using Java cryptographic libraries. In both cases, AWS Key Management Service is used for encryption key storage and management (rotation). Additional details are provided under Security Architecture

Application Architecture Component Services

The system leverages the existing FCS cloud environment using VPCaaS. The system includes its own hosting of CI/CD capabilities and environments for development, testing, UAT, staging (pre- prod) and production. The system also leverages existing GSA IT capabilities including GSA CAF Webservice, DSS, GSAuth, GEIP to implement various parts/features of the system.

User Interface using React

React provides a robust user interface support to provide a unified interface for the different business capabilities. React is a Javascript framework and can be served as a download from an S3 bucket. This will allow sensible use of a content delivery network solution.

API services using AWS API Gateway

Provides a comprehensive interface to the enterprise through an API gateway.

Microservices using RESTful interfaces

Each capability component along with the CRUD layer is exposed via RESTful interfaces used within the PPM solution. Java with Spring Boot and Spring Data provide these RESTful interfaces.

Containerization Serverless using AWS EKS, Docker Containers & AWS Lambda

Software is developed to run in a Docker/Containerd ecosystem. EKS manages the Docker based containers with EKS nodes supported by auto-scaling groups to

elastically scale on demand. Application load balancers mediate service calls between running containers. Lambda is used to provide simpler supporting services.

Data Storage using RDS Aurora (MySQL), RDS MySQL & S3

Production instances use traditional RDS MySQL in a High-Availability configuration for 24x7 operation. PPMS infrastructure also uses Amazon Aurora MySQL for non-production environments where the databases will automatically start up, shut down, and scale capacity up or down based per application's needs; lowering cost. S3 object stores provide PPMS a durable file system for data analytics operations, like ETL or map-reduce.

Integration with external systems using Apache Camel

Apache Camel (Java libraries used by the PPMS code) is used to integrate PPMS with other existing systems such as Pay.gov, GSA CAF Webservice, providing a unified way to interfacing with any system.

Data Transformation, Warehousing and Visualization using AWS Glue & Kafka

AWS Glue ETL service transforms/abstracts data in the PPMS RedShift data lake. AWS Glue automatically handles provisioning, scaling and configuration required to run the jobs. PPMS provides RedShift and Tableau services.

Security Encryption using AWS KMS & TLS Certificates

Provides a centralized way of creating and managing cryptographic keys to encrypt data “at rest”. PPMS requires credit card information to be stored, and the data is stored in an encrypted manner to meet the PCI-DSS requirements. Data “in flight” is encrypted using TLS 1.2 or 1.3.

Integration with FCS AWS for Bedrock

PPMS will integrate with Cohere Embed English and Claude Sonnet 4 models from AWS Bedrock for Embedding and Generative AI capabilities. The integration would utilize AWS Access Key Id and Secret Access Key which is managed by FCS.

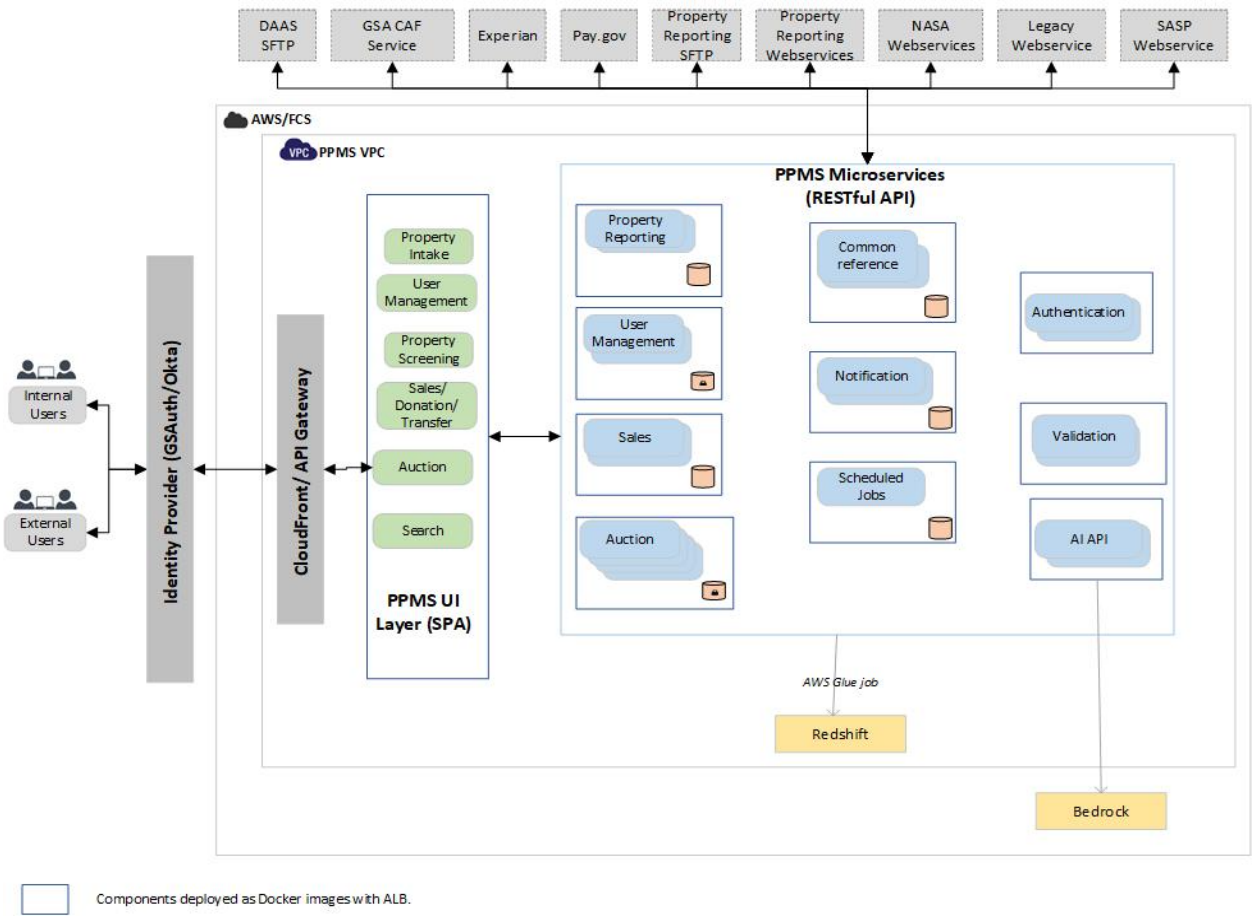

Figure 3: PPMS Architecture

1.0 Purpose of Collection

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

- 1878.2A CIO P Conducting Privacy Impact Assessments (PIAs) in GSA: This directive establishes policy and procedures for addressing privacy issues in GSA Information Technology (IT) systems, online Web sites, and social media venues containing personal information about individuals.
- 2180.1 CIO P GSA Rules of Behavior for Handling Personally Identifiable Information (PII): This directive provides GSA's policy on how to properly handle PII and the consequences and corrective actions that will be taken when a breach has occurred
- Privacy Act of 1974; Revised Privacy Act System of Records
- OMB M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- 40 U.S.C. § 521- Requires GSA to prescribe policies and methods to maximize the reuse of excess property. The implementing regulations can be found in FMR 102-35 and FMR 102-36.
- 40 U.S.C. § 545 - Requires GSA to sell property in accordance with this statute. The implementing regulations can be found in FMR 102-38.

- 40 U.S.C. § 549 - Authorizes GSA to transfer surplus property to State agencies for subsequent donation to eligible recipients. The implementing regulations can be found in FMR 102-37.
- E.O. 12999 - GSA hosts a website that enables agencies to transfer excess computer equipment to schools and educational non-profits under the Stevenson Wydler authority. https://computersforlearning.gov/htm/hp_eo12999.htm

The Federal Property And Administrative Services Act of 1949. The act was designed, in part, to increase the efficiency and economy of Federal government operations with regard to the procurement, utilization and disposal of property.

The Federal Property And Administrative Services Act of 1949 Section 484 - "Disposal of Surplus property" Provides that the care and handling of surplus property pending its disposition, and the disposal of surplus property, may be performed by GSA or any executive agency designated by the Administrator.

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/FSS-13 SORN applies to IQ-PPMS.

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.
Content in this system will be disposed according to the following GSA schedule:
137.3/021 Personal Property Case Files And Summary Reports. This series describes those records created when accounting for individual instances of managing the evaluation, processing, sale, and transfer of excess and personal property. Included are personal property sales case files (containing routine documents associated with the above-listed activities), excess and personal property catalogs, bulletins, and lists, utilization surveys, donation case files, reserve excess property files, rehabilitated property stock listings and reports, and related records.
Retention Instructions:
Temporary. Cut off at the end of the fiscal year when the property case file or transaction is completed and the final payment is received. Destroy 6 fiscal years after cutoff. Longer retention is authorized if needed for business reference purposes, but no longer than 10 fiscal years after cutoff.
Legal Disposition Authority:
DAA-0137-2015-0001-0010 (137.3/021)
Approved by NARA:
4/5/2018.

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?

The collection of PII is necessary for the PPMS mission because:

1) We need to confirm the eligibility of bidders. (Are bidders 18 or older? Are they restricted from doing business with the government? Are they in debt to the government?)

2) Debt Collection Improvement Act of 1996. In accordance with Public Law No. 104-134, Section 31001, The Debt Collection Improvement Act of 1996, the Tax Identification Number (TIN) must be provided by anyone conducting business with the Federal Government, from which a debt to the Government may arise. Individuals cannot successfully register to bid on items without providing a TIN. A TIN is defined as an individual's Social Security Number (SSN) or business entity's Employer Identification Number (EIN). TIN validation also assists in the prevention of fraudulent bidding activity and ensures that bidders are prepared to accept responsibility for their bidding activity and all submitted bids are valid.

3) If bidders default on a sales contract, we put them in default, and if it remains unpaid, all of their PII is securely made accessible to the U.S. Treasury so the debt can be collected. GSA sends this information to the Treasury Department via secure system-to-system API calls. No Treasury Department user has access to PPMS. Any PII that is made available to the Treasury Department is via GSA Finance Office for payments that are in default under the Debt Collection Act. All other PII information made available would likely be from the individual and any agreement or information that they have provided via their credit card company. We do not otherwise forward anything directly to the Treasury.

4) PPM sends a majority of our communication through email, but needs their phone number in case we are not able to contact them.

3.2: Will the system, application, or project create or aggregate new data about the individual?

Yes

3.2 Explained: If so, how will this data be maintained and used?

PPMS will use past bidding history data based on product categories to identify target users to send marketing emails for upcoming sales. The bidders will be selected by random (50% sampling) where marketing emails will be sent on a daily basis. The results will be used for marketing purposes only. The data will not be used to determine bidder patterns, behavior, and aggregate or derive additional data about the user.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. PII Data is secured at rest by: PANs are Key encrypted AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption. Pay.Gov Secures their cardholder data environment and complies with PCI DSS requirements

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

Public

3.4 Explain: Please elaborate as needed.

Access to sensitive PII and Credit Card information by system users will be logged, monitored and audited. This will be used for FISMA and PCI DSS compliance. IP Address information will be stored during bidding, payment, and registration and is infrequently used by law enforcement in cases of actual or suspected fraud.

3.5 What kinds of report(s) can be produced on individuals?

Access to sensitive PII and Credit Card information is logged, monitored and audited. This is used for FISMA and PCI DSS compliance. These logs are only available to system administrators.

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?

The Sales module produces Top 3 bidder report, register of remittance report, successful bidders report, defaulted bidders list.

- Top 3 bidders report: This report is produced for each sale/lot after the sale/lot is closed. The report lists the top 3 bidders for each sale/lot. The PII listed on this reports include bidder name, bidder company name (when available), address, email address, bidder #, and phone #.
- Register of remittance (ROR) report: This report is produced for every register (where payments are posted). ROR is an on-demand report which could be generated anytime after registers are closed. The PII listed in the report includes bidder name and last 4 of credit card # (for payments via credit card).
- Successful bidders report: This is an on-demand report which could be generated anytime after registers are closed. The PII listed in the report includes bidder #, bidder name and address.
- Defaulted bidders report: This report could be produced anytime. The report lists bidder # and bidder name.

All reports are accessible to the GSA Sales office as well as GSA-IT staff supporting the SASy module.

Auctions Reports: The application does not produce any report with PII information.

Sales Reports: The application does not produce any report with PII information.

Payment Reports: The application produces one report which is receipt of the payments made. The receipt prints payment details including payee name.

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?
Private-Sector Organizations

4.2How: If so, how will GSA share the information?
The Personal Property Sales program SORN states “System records include: (1) Personal information provided by bidders and buyers, including, but not limited to, names, phone numbers, addresses, Social Security Numbers, birth dates and credit card numbers or other banking information, and (2) contract information on Federal personal property sales, including whether payment was received, the form of the payment, notices of default, and contract claim information.

Information will be shared with Experian as minimally required to verify bidder identity and suitability for bidding.

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?
Auctions - Experian. The Auctions module shares bidder (Individual and Company) information for identity verification with Experian via the secure HTTPS PreciseID and BizID services. Data is transmitted electronically via a HTTPS service during user registration. The sharing of information is for the sole purpose of verifying the potential user’s identity so as to provide access to Auctions platform. A contract (Experian Data Use Addendum (DUA) to PO 4102859563 executed.pdf) is in place with Experian to provide PreciseID and BizID identity proofing services. The DUA document defines security and sharing parameters for information shared with and received by Experian. Experian will notify GSA of a suspected or confirmed security incident or breach of PII via email to the “HEAD SECURITY DESIGNATE” on file and other agency POCs as appropriate.

The Auctions, and Payment modules use Treasury’s Pay.gov interface to process payment for awarded auctions/sales. Agreements “Pay.Gov GSA Auction ACT 082304 revised.doc” and Pay.Gov GSA Auction ACT 082304 revised.doc are in place with the Treasury to provide electronic payment services. Treasury will notify GSA of a suspected or confirmed security incident or breach of PII via email to agency POCs on file and other agency POCs as appropriate.

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?

The source of the data is the individual providing the data during registration, payment, or profile updates. Identity data is verified on Auctions via Experian PreciseID and BizID services. If that fails, users can manually verify their identities with the Office of Personal Property Management. Email addresses, and email address changes are validated by an email activation link that is sent to the provided email address that the individual must click.

Auctions implemented identity proofing services to ensure that identity data provided by users was accurate and primarily not fraudulent. Experian services were chosen due to cost, ease of implementation, and Experian success providing similar services to other agency customers. These services mitigate risks associated with users attempting to register with another individual's information.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

Sales: GSA Office of Personal Property Management employees with system administration access, Auctions Help Desk GSAContractors with Help Desk role, and GSAIT Development team members have access to PII data. New system users with privileged access must fill out a system specific User Access Request form which is reviewed and electronically signed by the account group owner defined in the Sales modules.

6.1b: What is the authorization process to gain access?

Access Request Process is filed in the google shared team drive. The account is then created with the following parameters:

- Only the roles and permission necessary for that individual's job function
- Restricted to least privileges necessary to perform job responsibilities

Privileges assigned are based on the individual's job classification and function

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.
10/26/2026

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The IA-PPMS system implements NIST Special Publication 800-53 Rev 5 controls for a Moderate system. All controls were assessed during the ATO process.

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?

All PPMS Modules have role based access where users with need to know have access to the system. All GSA personnel undergo an annual Privacy training to ensure user privacy is maintained. Certain privileged users in Sales and Auctions applications have access to users SSN/TIN and credit card information. These privileged users' activities are logged as a security measure.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

Furnishing a social security number or tax identification number, as well as other data is voluntary, as is participation in the Personal Property Sales Program. Failure to provide this information, however, may result in ineligibility to purchase Federal personal property from the General Services Administration.

The Auctions Terms and Conditions (T&C) provides a statement on the need to collect Social Security Number for Individuals and Tax Identification Number (TIN). Text provided from Auctions T&C. The Debt Collection Improvement Act of 1996 is also referenced in the T&C as well as for fraud purposes. Credit Cards (CC) are not required to be provided during registration, however if a bidder needs to pay using CC, they have to provide one. Other PII information is required for all applications in order to validate user identity as well as have accurate user information.

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.

The Debt Collection Improvement Act of 1996 is also referenced in the T&C as well as for fraud purposes. Credit Cards (CC) are not required to be provided during registration, however if a bidder needs to pay using CC, they have to provide one. Other PII information is required for all applications in order to validate user identity as well as have accurate user information.

7.2: What are the procedures that allow individuals to access their information?

Auctions and Payment provide a “Protecting Your Privacy” web page which has a Privacy & Security Notice section that references the Privacy Act of 1974 (5 U.S.C. Section 552a, as amended). All other users have system use notification.

7.3: Can individuals amend information about themselves?

Yes

7.3How: How do individuals amend information about themselves?

Users can login to the system and update their information. They can also contact the respective point of contacts to update their information.

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.

All GSA staff and contractors are required to take the mandatory annual Privacy training. GSA IT produces a report to identify individuals who have not taken the training and ensure the training is completed by everyone. GSA/ISP provides annual privacy training to all GSA employees (both federal and contractors).

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?

Personal Property Management System (PPMS) is designed with role-based access. The business line determines and assigns application roles/permissions based on business need and need to know basis. During the User Access Request and Approval process, access forms are reviewed, signed and filled out to ensure that roles requested are the roles and permissions that are used for account creation.

Users provided access to the applications can access limited functionality based on user roles. External users do not have privileged access to any applications.

Audit Safeguards: The PPMS application is hosted in AWS Virtual Private Cloud within the GSA network. The server has access to authorized personnel for application support. The application boundaries are defined in PPMS SSP. The PPMS application is accessible via internal to its users.