

General Services Administration



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.

PIA

General Information

PIA ID:	PIA-481	PIA Status:	Completed
System Name:	GSA Real Estate Sales (GRES)		
Export PIA:	Yes		
CPO - Approval Date:	9/11/2024		
PIA Expiration Date:	9/11/2027		

Stakeholders Approvals

Information System Security Manager (ISSM) Approval

Name (Full)

Carolyn Campbell

System Owner / Program Manager Approval

Name (Full)

Jacob Panyko

Chief Privacy Officer (CPO) Approval

Name (Full)

Richard Speidel

PIA Overview

A.System Name:	A. System, Application, or Project Name:	GSA Real Estate Sales (GRES)
B.Includes:	B. System, application, or project includes information about:	
C.Categories:	C. For the categories listed above, how many records are there for each?	
D.Data Elements:	D. System, application, or project includes these data elements:	
Overview:	A: GSA Real Estate Sales (G-RES) B: Federal employees, contractors, and the public. C: Roughly 50-100 records unique of Federal Employees as they are the real estate specialists and system users. And roughly 1,000-10,000 subscribers/bidders - however, please note this is a public website and this number could greatly fluctuate. The number should similarly reflect what is close to the existing auction website. D: For the public: the collection of PII is necessary for the GSA Real Estate Sales (G-RES) to verify the identity and age of bidders who are bidding on listed real property. Bidders must be at least 18 years of age. Bidders will be required to provide their birth date at registration. A bidder's birth date will be used only to verify bidder's eligibility. The information will be traveled from Login.gov and to G-RES. For internal users: formation is necessary to create their accounts in G-RES to list properties and administer auctions. GSA real estate agent/specialist and GSA subdomain administrators profiles may contain first and last names, email, phone number, and address. This information is necessary to create their accounts in G-RES to list properties and administer auctions. Overview: G-RES is an online auction application that enables GSA's Office of Real Property Disposition (RPD) to sell surplus federal land, improvements to land and rights to land to the general public via the website https://www.realestatesales.gov . The auctions allow all registered participants to bid on property within specified timeframes. The online capabilities provide transparent competitive bidding, photos, videos and facilitates the sale of properties located across the country to any interested buyer, regardless of location or time of day.	

1.0 Purpose of Collection

PIA-1.1:	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?	Federal Property And Administrative Services Act Of 1949, As Amended Pub. L. 152, Ch. 288, 63 Stat 377 (Codified as amended in scattered sections of 40 U.S.C. and 41 U.S.C.) The General Services Administration (GSA) can dispose of federal property that is no longer needed through a process called Public Benefit Conveyance (PBC). PBC allows the GSA to give surplus land and buildings to public entities for free. The GSA can also sell surplus property to the public through competitive sales.
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	New SORN required
	PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-1.2 System of Records Notice(s) (Legacy Text):	What System of Records Notice(s) apply/applies to the information?	A new SORN is being drafted concurrently under the number GSA/PBS-11.
PIA-1.2b:	Explain why a SORN is not required.	
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.	
PIA-1.4:	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.	G-RES records will be kept in accordance with the GSA Records Retention Schedule. This retention schedule is part of a comprehensive Records Management overhaul of all of GSA's previous records (relating to agency mission-related work) and, simultaneously, those efforts of the National Archives and Records Administration (NARA) in a comprehensive overhaul of the General Records Schedule; used by all Federal Agencies in common tasks.

2.0 Openness and Transparency

PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2.1 Explain:	If not, please explain.	

3.0 Data Minimization

PIA-3.1:	Why is the collection and use of the PII necessary to the project or system?	<p>The collection of PII is necessary for the GSA Real Estate Auction Site (G-RES) to verify the identity and age of bidders who are bidding on listed real property. Bidders must be at least 18 years of age. Bidders will be required to provide their birth date at registration. A bidder's birth date will be used only to verify bidder's eligibility. This information is protected by the Privacy Act, 5 U.S.C 552a. In addition, bidders must not be debarred from doing business with the Government. GSA will verify that individuals and companies are not debarred by checking their information against the bidders debarred list which identifies those parties excluded throughout the U.S. Government (unless otherwise noted) from receiving Federal contracts or certain subcontracts and from certain types of Federal financial and non financial assistance and benefits. For complete information on parties excluded from doing business with the United States Government go to http://www.sam.gov. GSA AuctionsSM also adheres to the practices prescribed by The Office of Foreign Asset Control (OFAC) of the U.S. Department of the Treasury with regards to the Specially Designated Nationals and Blocked Persons List (SDN).</p> <p>GSA real estate agent/specialist and GSA subdomain administrators profiles may contain first and last names, email, phone number, and address. This information is necessary to create their accounts in G-RES to list properties and administer auctions.</p>
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	Yes
PIA-3.2 Explained:	If so, how will this data be maintained and used?	The only new information aggregated about an individual will be their bidding activity on respective real property listing(s). Although the bidder's name appears as a randomly generated numerical ID to other bidders during the auction, these IDs will be stored in the G-RES databases against the corresponding bidder's name and registration account. This bidding information is not shared with other systems and is used for historical audit purposes only.

<p>PIA-3.3:</p>	<p>What protections exist to protect the consolidated data and prevent unauthorized access?</p>	<p>Protecting data and prevent unauthorized access is paramount in the modern era. Therefore, G-RES utilizes and is not limited to the following:</p> <p>This information is encrypted in-transit and at rest and is only accessible to G-RES system administrators and PBS real estate specialists to view auction winners and conduct real property closings.</p> <p>A firewall is utilized to analyze and report network-related activities. Auditable events are captured through an audit aggregator, which is then forwarded for additional analysis to the appropriate system.</p> <p>Required cloud-native security services are configured to provide real-time monitoring and alerting capabilities. Automated alerts are triggered in response to security events, anomalies, and policy violations, enabling rapid incident response and remediation to mitigate potential security risks.</p> <p>Intelligent threat detection is enabled to detect and respond to threats in real-time by analyzing VPC flow logs, DNS logs, and event logs. This intelligent threat detection capabilities help identify suspicious activities, unauthorized access attempts, and potential security breaches, allowing for timely incident response and mitigation.</p> <p>G-RES also utilizes container scanning. The G-RES vulnerability tool continuously monitors running containers and server less functions in real-time, detecting and responding to security threats, anomalies, and policy violations.</p> <p>Web real-time applications logs are forwarded to the GSA managed SIEM through end point security. Event types include Web requests and responses, application administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. The endpoint security filters performance metrics and application log data that provide visibility to the GSA SOC, which is acting as a Security information and event management (SIEM) for GSA.</p>
<p>PIA-3.4:</p>	<p>Will the system monitor the public, GSA employees, or contractors?</p>	<p>None</p>
<p>PIA-3.4 Explain:</p>	<p>Please elaborate as needed.</p>	<p>The G-RES system does not currently have any integrations that would indicate debarment status for potential bidders. This will be done manually via the business line until SAM.gov integration in 2025.</p>
<p>PIA-3.5:</p>	<p>What kinds of report(s) can be produced on individuals?</p>	<p>Currently reports only list current users and the users statuses.</p>
<p>PIA-3.6:</p>	<p>Will the data included in any report(s) be de-identified?</p>	<p>No</p>
<p>PIA-3.6 Explain:</p>	<p>If so, what process(es) will be used to aggregate or de-identify the data?</p>	

PIA-3.6Why Not:	Why will the data not be de-identified?	The reports will not be de-identified, however real estate owners are public information obtainable from the Clerk of Courts in any county/state in the United States.
------------------------	---	--

4.0 Limits on Using and Sharing Information

PIA-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
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	None
PIA-4.2How:	If so, how will GSA share the information?	
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	What is the other source(s)?	
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes
PIA-4.4Who How:	If so, who and how?	<p>The interface with Login.gov will authenticate G-RES subscriber accounts using a user provided email account and will validate users' identities for bidder accounts with required personal information.</p> <p>The interface with GSA SecureAuth verifies the identity of internal GSA employees for access to G-RES.</p> <p>The interface with ESRI is used for geolocator services for listed real property in G-RES</p> <p>The platform is connected to the AWS Simple Email Services (SES) facilitating seamless communication and the efficient flow of information between the platform and department personnel. Once the Lightweight Authority to Operate is approved by GSA and access is granted to GSA GoogleMail, the plan is to switch from SES to Gmail.</p> <p>(Planned) The interface with SAM.gov will check the users' names and/or company names against the public debarment list.</p>
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	Yes
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	G-RES currently verifies users with the utilization of Login.gov identity verification. G-RES contains no data input fields for PII. Additionally, all user PII originates with Login.gov for all subscriber and bidder (privileged) accounts. PII data fields obtained from Login.gov, are displayed in G-RES, but they are "greyed out" and are not editable by the user. If the user wishes to change any PII data, they will have to change it in Login.gov, not G-RES.
-----------------	--	---

6.0 Security

PIA-6.1a:	Who or what will have access to the data in the system, application, or project?	<p>AWS accounts for the G-RES team are created with account access as either FullAdmin, SysAdmin, or ReadOnly.</p> <p>The G-RES application has various types of users depending on business needs such as: viewer, subscriber, bidder, realty specialist, and SubDomainAdmin.</p>
PIA-6.1b:	What is the authorization process to gain access?	<p>For G-RES internal GSA accounts, this is handled internally with multiple organizations within GSA. Documentation will be required in order to request an account. Additional FISMA requirements will need to be complete in order to ensure security compliance.</p> <p>For external accounts, this will be handled through the G-RES application in the aid of Login.gov.</p>
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	
PIA-6.3:	How will the system or application be secured from a physical, technical, and managerial perspective?	G-RES abides by and not limited to: all GSA CISO, FIMSA, NIST, and CISA requirements ensuring confidentiality, integrity, and availability.
PIA-6.4:	Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?	Yes
PIA-6.4What:	What are they?	AWS security tools, container security tools, and log security tools are used to identify and respond to suspected or confirmed security incidents and breaches of PII.

7.0 Individual Participation

PIA-7.1:	What opportunities do individuals have to consent or decline to provide information?	Individuals may use G-RES as "view only" as a public, non-registered, non-privileged user. If they chose to register for a subscriber or bidder account (privileged user), they must agree to input the required information into Login.gov. If they decline to enter the required information into Login.gov, they will not be granted a privileged account.
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7.1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
PIA-7.2:	What are the procedures that allow individuals to access their information?	Individuals input their personal information into Login.gov for identity verification in G-RES. Login.gov then sends that user entered information to G-RES. In G-RES, individuals only have "read only" access to their information. If they want to change their personal information, they would have to go back to Login.gov. Users cannot directly change their personal information in G-RES.
PIA-7.3:	Can individuals amend information about themselves?	No
PIA-7.3How:	How do individuals amend information about themselves?	

8.0 Awareness and Training

PIA-8.1:	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	All GSA employees and GSA contractors are required to take yearly IT Security & Privacy Awareness Training.
-----------------	--	---

9.0 Accountability and Auditing

PIA-9.1:	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	The G-RES system owner will support all GSA's Quarterly Performance Metric Reviews (PMRs), and will be performing annual FISMA Self Assessments.
-----------------	---	--