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: 395
System Name: Pegasys Vendor Request Management (VRM)
CPO Approval Date: 10/12/2022
PIA Expiration Date: 10/11/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Jennifer Hanna

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Pegasys Vendor Request Management (VRM)

B: System, application, or project includes information about:
Vendors and federal employees

C: For the categories listed above, how many records are there for each?
43,095 total count

D: System, application, or project includes these data elements:
Application includes traveler name, addresses, telephone numbers and email addresses, SSN for travelers, bank routing number, account numbers and TINs. Vendor Request Management can also store information for employee travel which is at the individual level. Employees can request to update information for travel.

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)-2, and 26 CFR 31.6109-1.

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?
Search by SSN, TIN, and DUNS.

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.
GSA has a NARA-approved records retention schedule. The financial data is retained for 6 years 3 months as required by NARA. An employee's historical records are maintained in the database for 18 months after separation and are then purged from the database. The Pegasys financial records are the system of record, but GSA currently maintains the ACA records indefinitely. At a minimum NARA requires retention for at least 6 years after contracts expire for financial management records. Financial records are retained per National Archives and Records Administration (NARA) standards for at least six years. The ACA records may be retained online longer for historical reviews, but at a minimum will be retained six years. Pegasys is the system or record for the financial data.

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?
PII collection is necessary in the Vendor Request Management (VRM) system to allow the submission of vendor requests be securely transmitted to vendor coding staff who create new and update existing vendors using the PII information. Payments to vendors would not be possible without the PII information. System does not provide notice to the vendor that they have been added to the system.

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?
The MySQL database used for the app is a standard configuration that implements TDE for at rest encryption and TLS 1.2 for in-flight encryption.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
None

3.5 What kinds of report(s) can be produced on individuals?
None

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
PII data in reports will be obfuscated with asterisks '*', similar to how password input fields are masked.

3.6 Why Not: Why will the data not be de-identified?

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?
GSA shares this information manually with USDA via Pegasys. VRM users utilize data received in VRM to make updates directly in the Pegasys system (owned by USDA) - no direct transmission from VRM to Pegasys.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Information is only collected directly from the source.

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?
USDA.

GSA shares this information manually with USDA via Pegasys. VRM users utilize data received in VRM to make updates directly in the Pegasys system (owned by USDA) - no direct transmission from VRM to Pegasys.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?
ISSO is to fill

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 manual input from Contracting Officers or their representatives. The data is then manually verified by vendor coders.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Requesters will have access to only their submitted data. No application role is required for this type of access. Vendor Coders can access request lists and search for specific requests to manually key into Pegasys. Vendor Coder Managers and VR COOP users can run reports in addition to having the same privileges as Vendor Coders. Roles that require approval (all except requester) are reviewed by the VRM System Owners following manager approval.

6.1b: What is the authorization process to gain access?
Vendor Coder Managers and VR COOP users can run reports in addition to having the same privileges as Vendor Coders. Roles that require approval (all except requester) are reviewed by the VRM System Owners following manager approval.

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.
8/31/2020

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The assets utilized for VRM are within a federal data center and secured appropriately. The application uses role based access managed through EARS, CAAM, and MFA. EARS (Enterprise Access Request System) users request access to systems, CAAM access is implemented, and MFA (Multi Factor Authentication) is used to authenticate to the application. MySQL database is encrypted at rest with column level encryption. Data in transit is encrypted via TLS 1.2.

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?
VRM leverages the GSA incident response guide. Any suspected incidents or breaches of PII are reported to IT Helpdesk. IT Helpdesk submits incident tickets which are forwarded to GSA incident response team and privacy office if potential PII exposure was involved.

7.0 Individual Participation

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

The vendor has chosen to opt in by doing business with GSA. GSA employees agree to provide their information in order to conduct travel. There is a PII policy but not a Privacy Act Notice/Statement.

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 information is used for vendor payments. Users can opt out by choosing not to do business with GSA.

7.2: What are the procedures that allow individuals to access their information?
The user can submit a request through ServiceNow for the individual record. Internal users and travelers can request information through ServiceNow. Outside customers can request information through customer support at 800-676-3690.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
To request a change to an existing vendor code, choose the appropriate service office and then input the vendor code under “Edit Existing Vendor.” If you know the specific address code, you may input that as well. If you do not know the address code, you will get a list from which to choose. Select the address code you want to change. After selecting the address code you want to change, a Review and Edit screen will come up. The screen will display the current information on the vendor address code. Click on Edit and the application will take you to the beginning screen to work your way through the screens and data you need to change.

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 employees are required to take the annual GSA Identifying and Reporting Incidents and Breaches and GSA Mandatory Cyber Security and Privacy Training. Contains PII. Required to take Reporting Incidents and Security Breaches. For users, there is a user guide under the Help section of the website. Aside from that, USDA Finance is not aware of any other front end user training. USDA Finance has VRM vendor coding training and desk guides for finance duties associated with processing VRM vendor requests (USDA Finance are the users)

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?
Audit logs, technical implementation, role based access, encryption. Third party parties conduct assessments.