Pegasys Vendor Request Management (VRM)

Privacy Impact Assessment (PIA)

July 21, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Jay Myung

Name of Program Manager/System Owner:

- Leo Yang

Signature Page

Signed:

DocuSigned by:

Jay Myung

9EA3582A35764F1...

Information System Security Manager (ISSM)

DocuSigned by:

Leo Yang

07839B77A72A409...

Program Manager/System Owner

DocuSigned by:

Richard Speidel

171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
6/9/2020	New PIA – Content Added	3.1
6/16/2020	Addressed Comments	3.2
7/21/2020	Updated Business Line Comments/Approved	3.3

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about Pegasys Vendor Request Management (VRM). To accomplish its mission The Office of the Chief Financial Officer (*OCFO)* must, in the course of managing vendor requests, 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]

A. System, Application, or Project Name:

Pegasys Vendor Request Management (VRM)

- FISMA system - GSA Ancillary Corporate Applications (ACA)

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

This application supports requests for new or updating existing Vendor Codes. Also supports the creation of Employee Travel numbers. Previously, vendor requests were sent through email, this application eliminated sending PII via unencrypted email. GSA employees don't travel to vendors. VRM provides a way for employees to setup a Pegasys vendor to allow reimbursement.

Vendor Request Management collects the following PII information for vendors: TIN, bank name, bank ABA number, bank account type, bank account number and SSN. It is used to verify that vendor information in Pegasys is complete. It is manually entered by a Contracting Officer or their representative. Vendor coders then verify the information.

VRM collects the PII via the front end GUI; authorized vendor codes pull the information from VRM and hand-key the information into Pegasys.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

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? If so, what System of Records Notice(s) apply/applies to the information?

- Yes, can search by SSN, TIN, and DUNS.

1.3 Has an 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.

- No - The information in these systems are not collected from the public and thus are not subject to the Paperwork Reduction Act.

1.4 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.

- 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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

- Prior to accessing the system, users are provided a warning banner which they must accept or deny. Only internal GSA users can access application

SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

- 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? If so, how will this data be maintained and used?

- No

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

- Virtual Private Database (VPD), a feature of Oracle Database Enterprise Edition, is used when the standard object privileges and associated database roles are insufficient to meet application security requirements. VPD policies were set in VITAP databases depending on GSA PII security requirements to enforce sophisticated column level security requirements for privacy and regulatory compliance.

VPD enhances internal control and facilitates a statistical sampling process to ensure vendor data integrity and detect possible fraudulent activity being performed when creating and modifying vendor records. If the user is unauthorized, no matter how the user connect to the protected table (via an application, a Web interface, toad, SQL developer, or SQL*Plus), the visible result is the same - NULL. The MySQL that is to be 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?

- No

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? 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.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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. VRM is only used by those submitting PII information on vendor requests and Finance vendor coding staff entering the information to update or create the vendor in our accounting system. In the accounting system as well as VRM, access to PII information is restricted using security roles which prevent those without a need to know from accessing.

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?

- GSA shares this information with the U.S. Department of Treasury in relation to payment files and debt collection files that are transmitted to the Treasury using Secure File Transfer Protocol (SFTP).

The application itself doesn’t share the data with the Treasury.

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)?

- 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? If so, who and how? Is a formal agreement(s) in place?

- No

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

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.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

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?

- 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.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

- VRM is included in the ACA SSP and roles are the same. ATO expected for new environment late July 2020, Early August, 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. Use role based access managed through EARS, CAAM, MFA (EARS- Enterprise Access Request System – users request access to systems, CAAM – access is implemented, MFA – Multi Factor Authentication 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? If so, 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.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

- 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's a PII policy but not a Privacy Act Notice/Statement.

7.2 What procedures 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 – 800-676-3690

7.3 Can individuals amend information about themselves? If so, how?

- Yes. GSA employees can submit travel vendor updates as well as submit an Update Request in VRM upon their customer's vendor code update request.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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)

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

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.

---

[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.