




Instructions**Privacy Impact Assessment (PIA)**

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

00 Default Layout**Workflow
Status:**

99 Workflow Complete

PIA**General Information**

PIA ID:	PIA-276	PIA Status:	Completed
Authorization Package (System Name):	Pegasys Vendor Request Management (VRM)	This is a RPA:	No
Assessment Date:	12/22/2021	Is Latest:	Yes
FISCAL Year:	2021	PIA Required (From Authorization Package):	Yes
Final FISCAL Year:	2020	PIA Expiration Date:	12/22/2022
		Final PIA Expiration Date:	12/22/2022

Override / Reopen Explanation

Override FISCAL Year:	2020	Override PIA Expiration Date:	
Reopened Explanation:	Please review.		

Other Stakeholders

Stakeholders (not in Approval Process)

System Owner (SO): Lawless, Joe J

Authorization Official: DelNegro, Elizabeth F

System Owner (eMail)

Name (Full)

Joe Lawless

Joe Lawless

Authorization Official (eMail)

Name (Full)

Elizabeth Delnegro

PIA Overview

A.System Name:	A. System, Application, or Project Name:	Pegasys Vendor Request Management (VRM)
B.Includes:	B. System, application, or project includes information about:	Vendors and federal employees
C.Categories:	C. For the categories listed above, how many records are there for each?	43,095 total count
D.Data Elements:	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:		
PIA-0.1:	Is this a new PIA or Recertification request?	Annual Recertification
PIA-0.1Changes:	If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?	No, Changes

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

1.0 Purpose of Collection

PIA-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)â€², and 26 CFR 31.6109â€²1.
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?	Existing SORN applicable
	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?	Search by SSN, TIN, and DUNS.
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.	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

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?	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.
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3.2 Explained:	If so, how will this data be maintained and used?	
PIA-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.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3.4 Explain:	Please elaborate as needed.	None
PIA-3.5:	What kinds of report(s) can be produced on individuals?	None
PIA-3.6:	Will the data included in any report(s) be de-identified?	Yes
PIA-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.
PIA-3.6 Why Not:	Why will the data not be de-identified?	

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?	Federal Agencies
PIA-4.2How:	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.
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	What is the other source(s)?	Information is only collected directly from the source.
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	No
PIA-4.4Who How:	If so, who and how?	
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	ISSO is to fill

5.0 Data Quality and Integrity

PIA-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

PIA-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.
PIA-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.
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.	8/31/2020
PIA-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.
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?	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

PIA-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. Thereâ€™s a PII policy but not a Privacy Act Notice/Statement.
PIA-7.1Opt:	Can they opt-in or opt-out?	No
PIA-7.1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	ISSO is to fill
PIA-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 â€” 800-676-3690
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-7.3How:	How do individuals amend information about themselves?	GSA employees can submit travel vendor updates as well as submit an Update Request in VRM upon their customer's vendor code update request.

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.	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

PIA-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.
-----------------	---	---