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: 352
System Name: Web Vendor (WV)
CPO Approval Date: 9/23/2021
PIA Expiration Date: 9/22/2024

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Leo Yang

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Web Vendor (WV)

B: System, application, or project includes information about:
Web Vendor is used by GSA vendors to search for their Purchase Orders, past and pending payments, status of invoices, and submitting new invoices electronically. This can only be used for invoices processed via VITAP. Web

Vendor primarily allows vendors to submit new invoices and search for invoices. It also allows vendors to search their purchase orders (i.e., to find the purchase orders they want to invoice) and pending payments. Vendors have the ability to view: submitted invoices pulled from VITAP and other data (i.e., payments) from Pegasys.

C: For the categories listed above, how many records are there for each?
For Web Vendor the following records are as follows:

Records counts for Vendors are approximately 25,000 accounts; Invoices are approximately 4 million and Payments are approximately 45 million.

D: System, application, or project includes these data elements:
Web Vendor subsystem includes these data elements which are Vendor (accounts): username, vendor name, email, TIN/pegvendcd Invoices: Vendor name and address, TIN/pegvendcd, amount, invoice number, contract/PO number, service period Payments: Vendor name, TIN/pegvendcd, amount, EFT/check number, invoice number, date paid

Overview:

The Web Vendor application allows GSA Vendors to search for their Purchase Orders (POs), past and pending payments, status of invoices, and to submit new invoices electronically.   Web Vendor can only be used for invoices processed via VITAP. GSA vendors access the application via the Internet. The vendors can create the electronic invoices only against the POs found in the Pegasys PO table. All the submitted information is saved in the VITAP database. The process is automated. Vendors submit the electronic invoice via the website and the details are saved to the VITAP database, and related images are stored on the web server. An automatic back-end process runs and imports these invoice details into the Pegasys Invoice Table in VITAP and moves the related image files to ImageNow. Web Vendor captures the following potentially personal data; Vendor Name, email, phone number, TIN numbers . The vendor name, phone, and email address only comes in as personal data where a vendor is a sole proprietor using their personal information for business purposes

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
48 CFR 1232.7002 Invoice and Voucher review and approval – provides for the collection of invoices for contracts and the review of these by the government for the purpose of receiving payments from vendors using Federal space and for receiving invoices for payment.

Vendors who use their SSNs rather than a Tax Identification Number (TIN) introduce personal data into ACA. ACA is used to manage financial processes that are geared towards Accounts Payable and Accounts Receivable workflows.

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?
ACA has a SORN that is under Pegasys, and Web Vendor is covered because it is a subsystem of ACA

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.
The information in these systems are not collected from the public and thus are not subject to the Paperwork Reduction Act.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Both Pegasys-related records and other CFO-related records are retained under General Record Schedule record series *Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting* (Disposition Authority: DAA-2013-0003-0001 (GRS 1.1, item 010). The record retention instructions for this series is: "Temporary. Destroy 6 fiscal years after final payment or cancellation, but longer retention is authorized if required for business use."

The ACA records, derived from Pegasys, will be retained for an additional fiscal year from the date of last payment (7 fiscal years), for historical review purposes, and then disposed of under the same record schedule (GRS 1.1/010).

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 ACA applications use the vendor information to connect the company with the purchases and/or the invoices in the financial system. Vendor POC information is used to communicate with vendors (phone and email) and the TIN is used as an identifier in the Pegasys financial system for reporting data to the IRS. The TIN is shown in these applications in order to authoritatively match with records in Pegasys since vendor names can have overlaps.

Privacy Risk: Is there a potential risk of PII being shared to Pegasys without authorization?

Mitigation: No. The only data from ACA that is shared with Pegasys is related to financial transactions. Pegasys contains the relevant vendor information.

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?
The applications do simple queries on the Vendor Code (usually a TIN) and names, but not detailed analysis or calculations. The applications do not perform complex analysis but users will match data and store new information. For example, Web Vendor allows users to submit an invoice against a matching purchase order. Another example is VITAP's ability to generate accounting entries based on submitted documents.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
ACA shares data with Pegasys through the VITAP interfaces with Pegasys. There is a signed Interconnection Security Agreement and Memorandum of Understanding between GSA and USDA for the data exchanges that occur. In particular the ACA applications obtain the vendor information (which can contain personal information) from Pegasys.

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

3.4 Explain: Please elaborate as needed.
The system does not collect any information in identifiable form (personal data/information) on government employees.

The system does collect information in identifiable form on the general public

The applications do not use data from commercial / public sources.

3.5 What kinds of report(s) can be produced on individuals?
The primary purpose of these applications is to allow end users to cross-reference data across financial applications and data. The accuracy is confirmed by these end users, not through automated means. The Pegasys system at USDA remains the authoritative source for financial transactions and these applications assist in the financial workflow

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?
The applications do simple queries on the Vendor Code (usually a TIN) and names, but not detailed analysis or calculations. The applications do not perform complex analysis but users will match data and store new information. For example, Web Vendor allows users to submit an invoice against a matching purchase order.

3.6 Why Not: Why will the data not be de-identified?
The applications do simple queries on the Vendor Code (usually a TIN) and names, but not detailed analysis or calculations. The applications do not perform complex analysis but users will match data and store new information. For example, Web Vendor allows users to submit an invoice against a matching purchase order.

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?
No

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Other Individuals

4.2How: If so, how will GSA share the information?
All MOUs are reviewed by the system owner, program manager, Information System Security Officer, Information Owner, and counsel and then sent to A&A Review Team for formal review.

ACA tracks the transmission of data to Pegasys in audit logs that contain information compliant with GSA’s audit log procedures.

The Pegasys SORN for GSA (GSA/PPFM-11) is being updated to indicate that Pegasys has moved to USDA and ACA shares data between the two systems.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
The ACA applications receive vendor data from Pegasys. Web Vendor users with administrative rights for their company can register other users from the company. The information captured for those users is their name and email address.

The data provided from ACA to Pegasys is not the personal data and is not shareable.

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?
Data is shared between this system and Pegasys. It is a two-way interface, but personal data is only shared from Pegasys to ACA. ACA does not provide updates of the personal data back to Pegasys.

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 applications that collect individual data ancillary to the billing and accounts receivable process and only where individuals are using personal information for business purposes. The records collected in ACA are related to invoices and accounts receivables. When companies are sole proprietorships and the owner does not have a separate Tax Identification Number (TIN) from the Internal Revenue Service that is not their Social Security Number (SSN), the records may contain multiple possible personal information to include: person's name, SSN, home address (if they do not have a separate business address), home phone, and e-mail address. The number of records containing PII is a small percentage of the overall record set and Pegasys has a process for replacing an SSN entered by a vendor with an "S" vendor code.
Analysis is performed by the user and not the application. The data analyzed is related to reconciliation of the information displayed in these applications versus data in the Accounts Payable or Accounts Receivable modules within USDA's Pegasys system.
Applications receive data from Pegasys as the official system of record for financial transactions. Data such as the vendor information can be retrieved from Pegasys. Therefore, the ways in which Pegasys handles the TIN or SSN determines which data is passed on to these applications as noted in Section 1 of this document. These applications can also flow data to Pegasys, for example, in the case of Web Vendor. The actual individual / personal information such as the vendor registration information is not passed on to Pegasys. The vendors must already be in the Pegasys system and that system is the authoritative source of the vendor information

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
GSA IT Employees from Corporate IT Services in the Financial Management Line of Business, USDA Finance users with Admin or Read-Only roles, and Vendors will have access to this information. Additionally, some VisualCron jobs will have access to this data.

6.1b: What is the authorization process to gain access?
Internal users (e.g Admin or Read-Only) request access to the system using GSA's Enterprise Access Request System (EARS). EARS forces the user to specify the roles they are requesting. Each request from a potential end user is reviewed by an approval workflow which complies with the GSA IT Procedural Guide for access control. The minimum workflow requires approval of the applicant's supervisor prior to a system administrator adding the user into the role requested.

The roles define whether the user has read-only or write privileges.

External Users (Vendors) request an account by entering a TIN number that already exists in the Pegasys System and verifying the Vendor information. The user then fills out a Registration Form that contains Name, Email, and Phone number. Once submitted, the internal Admin verifies the account and creates the Username.

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.
10/1/2021

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Role-based access is applied and enforced so personal data cannot be exposed to individuals who do not have a need to know.
The ACA applications are in a Moderate FISMA boundary with role-based access that is reviewed by system owners.
An interconnection agreement is in place with USDA for the Pegasys system to share vendor information with ACA. This ensures a secure connection with only the data required being shared between the two systems.
Any PII for ACA has been encrypted at rest utilizing TDE

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?
Audit log reviews are performed when suspicious activity is detected or a security incident has been reported. Audit Log reviews are performed on at least a weekly basis by ISSO. Additionally, DBA's monitor access to databases.
ACA follows the GSA IR Guidance 01-02.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Individuals do not use the applications that are the subject of this PIA. The individuals whose data is captured in ACA consent to use their information when signing contracts with GSA or leasing GSA facilities. The data collected is intended to be vendor data and it is the individual’s choice to use their personal information instead of applying for a company Employer Identification Number from the IRS. Individuals should consider using a TIN instead of their personal SSN when doing business with the government. The IRS covers this in their guidance to self-employed individuals -
https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin and GSA makes this information available to vendors during the process.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?
Individuals should contact the ACA Information Owner with questions regarding any of their personal data in the system.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Discrepancies in data must be corrected in Pegasys and then the corrected data will be migrated back to ACA.
Privacy Risk: If users in Pegasys enter the vendor data incorrectly, that data will be incorrect in ACA as well. The ACA applications are used primarily for tracking and matching data. The process is not visible to the individuals except through contracts that use Web Vendor for invoicing.
Mitigation: The contracting / ordering process and associated documentation is the individual's window into the financial records and processing. Each vendor should check the accuracy of the purchase order documentation as it relates to any personal information. For information on gaining access and working with Web Vendor, refer to the Frequently Asked Questions.
Vendors are made aware of accounts payable and accounts receivable processes through their contracts. For disputes or corrections, they would contact their Contracting Officer / Specialist and follow the procedures in the orders they receive.

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 Federal Government employees and contractors receive annual general security awareness and privacy training. This is relevant to how ACA records are handled and users are trained to understand the importance of protecting the records and documents stored in the system.

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 reviews are performed at the operating system level to identify any anomalies of server-level activities. The application logs may be reviewed if an incident occurs. Database and application logs are reviewed by ISSO on at least a weekly basis.
Training and documentation in Pegasys covers the use of the vendor code field and the use of the "S" in the code for vendors using their SSN while doing business with the government. This information is also covered in the user guide information for the applications and all ACA users must complete privacy and security training on an annual basis.