



Ancillary Corporate Applications (ACA)

Privacy Impact Assessment (PIA)

April 22, 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:

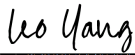
- Leo Yang


Signature Page

Signed:

DocuSigned by:

9EA3582A35764F1...
Information System Security Manager (ISSM)

DocuSigned by:

07839B77A72A409...
Program Manager/System Owner

DocuSigned by:

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
2/20/2020	Removed email field from signature page	3.1
4/20/2020	Updated – New Template	3.2

4/22/2020	Approved	3.3

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 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.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

SECTION 4.0 LIMITS ON USES AND SHARING OF 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, maintenance, use, or dissemination?
- 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?
- 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)?
- 4.4 Will the system, application, or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

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 Ancillary Corporate Applications (ACA). To accomplish its mission GSA IT must, in the course of ACA 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:

See Overview

B. System, Application, or project includes information about:

Federal employees, contractors, the public

C. For the categories listed above, how many records are there for each?

See Overview

D. System, application, or project includes these data elements:

See Overview

Overview

The GSA Ancillary Corporate Applications (ACA) system is operated by the Office of Corporate IT Services, FM & HR IT Services Division. The system boundary includes the ancillary systems that support the financial functions of Pegasys, Legacy National Electronic and Accounting Reporting (NEAR) historical data and Financial Management Information System (FMIS), all of which are owned and managed by USDA. These ancillary applications assist in GSA's mission by allowing the Office of the Chief Financial Office users to review, validate, and reconcile transactions in a variety of financial domains such as vendor invoices and accounts payables.

Overview

The GSA Ancillary Corporate Applications (ACA) system is operated by the Office of Corporate IT Services, FM & HR IT Services Division to support the financial management process which primarily occurs in the United States Department of Agriculture (USDA) system known as Pegasys. GSA's Associate Chief Information Officer of the Office of Corporate IT Services is the Authorizing Official of ACA and all the minor applications that fall under this system. The applications facilitate the financial management processes to improve efficiency and accuracy of the transactions in Pegasys, but none of the applications within ACA are the authoritative financial records.

The following are the applications within ACA that contain data subject to the Privacy Act (Personally Identifiable Information – PII). The summary of each application describes the PII data that is collected and the method(s) of collection.

- **Concessions Accounts Receivable System (CARS)** - This application provides read-only access to historical records and no changes are made to the data. In the past CARS, provided accounts receivable tracking, report generation, and management information for concession leases. CARS handles accounting for concession related income (e.g., a cafeteria within a government public building). The amount recorded in CARS is the amount of the check paid by the concession holding company. Personal data may be collected in CARS if a concession is run by an individual as opposed to a company. The system collects the name and address of the concession payer.
- **Check Cancellation** – Check Cancellation is a read-only application and provides historical data. The Check Cancellations application was previously used by GSA personnel in the Kansas City Finance Center to import check cancellation files from Treasury and provide data for associates to make appropriate accounting entries. This data was also used in the cash reconciliation process performed by the Pegasys Finance Branch. The data is viewed in Check Cancellation application and compared to Pegasys Cash transactions. Additionally, the application exports

a daily Excel file which is manually sent to a mailing list of individuals who require this data to perform their job functions (e.g., GSA accountants). If GSA receives checks from individuals (sole proprietors using their name and personal banking information) then the name and bank account information would be personal data. Most of the transactions however are related to companies and include only company data.

- **Federal Supply Service Payment System (FEDPAY)** - The Federal Supply Service Payment System (FEDPAY) provides an automated method for electronically receiving and processing Federal Supply Service purchase orders as well as the subsequent processing of vendor-submitted invoices against those purchase orders. For each invoice processed for payment the FEDPAY system creates a billing record that is passed to the Federal Acquisition Service Pegasys Connect for generating billing records to customers. The FEDPAY system receives all purchase orders electronically from interfacing systems. Vendors may submit invoices to FEDPAY via the Internet, Electronic Data Interchange (EDI), or through the mail. The FEDPAY system consists of user-friendly online menu items, update forms, query forms and reports to input, process, and retrieve transactions easily and quickly such as purchase orders, invoices, claims, receipts, and vendor information. Like other ACA applications, the only personal data collected in FEDPAY occurs when a vendor provides personal information for example if they are a sole proprietor using their name and address for the company. Most of the transactions however are related to companies and include only company data.
- **Invoice Search** - Invoice Search is an application that searches for invoices in the Visual Invoice Tracking and Payment (VITAP) system to track paid and delinquent (over 20 days old) invoices. The application allows users to view outstanding and paid invoices in the VITAP and Pegasys systems, view images of invoices, and reject invalid invoices via the web (rejecting an invoice does not delete data, it simply marks it as a rejection. Follow up is then performed to ensure that the invoice is invalid). Users cannot modify data using Invoice Search. It relies on user roles within Pegasys for authentication and the data visible to the user is filtered based on his/her Parent Organization (e.g. GSA). This application provides a key piece of the agencies' overall Accounts Payable workflow process. Invoice images displayed in Invoice Search may contain PII such as addresses, phone numbers, Taxpayer Identification Numbers. The application also displays bank information which could be an individual's if they do not separate their personal and business banking information. Invoice Search does not distinguish personal and business accounts and the same protections are applied to both categories of information.
- **Outlease Accounts Receivable System (OARS)** - This application provides read-only access to historical records and no changes are made to the data. GSA outleases space when a long-term Federal rental need is identified but full

utilization of the space is not achievable in the short-term. OARS creates coupon books and tracks receipt of outlease rents in Federal buildings, handles special charges (e.g., cleaning) for a building, and creates sales accounting entries for each income type when an outlease occurs. OARS provides accounts receivable tracking, report generation, and management information for Public Building Services (PBS) leases to non-federal customers. The application can generate monthly receivables reports, reverse out deferred liabilities in the large beginning of month batches, and track the payments of individual accounts on a month by month basis, report on the inventory of spaces being leased by each region, and produce delinquency report on overdue accounts. In addition, OARS has the ability to track the leasing of Historic Buildings separately. OARS processes and records data that could be used to identify individuals such as billing names, addresses, contract numbers, and history of payments.

- **Pegasys Online Disbursement Review (POLDR)** - Pegasys Online Disbursement Review (POLDR) provides the Financial Operations Division a consolidated view of matched documents including purchase orders, receiving reports, invoices, and payment authorizations in order to expedite the approval or disapproval of payments in Pegasys. POLDR pulls together all four views into four quadrants of a single screen so that the Financial Analyst can review the Payment prior to certification. Users review invoice, purchase orders, receiving reports, information from payment documents in Pegasys within the four quadrants. Users review documents to approve or cancel payments. When a payment is approved, the approval is linked to a scanned image from VITAP to copy the actual invoice. The approval occurs in POLDR and is then sent to Pegasys. VITAP feeds information into POLDR. If a payment is rejected, it creates an exception in VITAP, so that the issue can be resolved by the Financial Analysts. POLDR displays data from Pegasys to include: Vendor Code/TIN , Vendor Address Code, DUNS Number, Vendor name, Remit to Address, Vendor Account Numbers, Invoice Number, Invoice Amount, Receipt acceptance data. POLDR contains vendor bank account information including account and routing numbers. The use of personal data is minimal but possible.
- **Utility Payment Profile System (UPPS)** - The Utility Payment Profile System was developed to track and pay GSA utility bills and create projections of future utility payments. UPPS produces a file of utility payment information for the PBS-IS EUAS system and provides a report that identifies utility bill payments that are out of tolerance with PBS building energy usage profiles. The application is used to process utility payments, setting up utility accounts, and paying invoices. UPPS is also used for setting up monthly profiles (monthly accruals). This application supports PBS and all utilities except telephone bills. UPPS technicians have scanners that scan the physical copies of bills from electric, water, and gas companies. These bills are usually received by mail for all GSA owned property. When invoice is received, payment is entered in UPPS to post. Then scanned in

batches, and then sent to Pegasys, through a VITAP output process. Pegasys feeds vendor information into UPPS. The data also contains invoice numbers and customer name. There is currently a plan to migrate the UPPS application to another 3rd party system.

- **Utilities System** - The Utility System was developed to track and pay GSA utility bills and generate projections of utility payments. It is a .Net Web application that provides access to the information in the UPPS tables. Utilities System allows users to query the UPPS tables in a read only mode. The application allows users to reconcile payments that are out of tolerance with PBS building energy usage profiles and random sample reports. Additionally the app is used for approximately one month a year to do updates to Payment Profiles used by UPPS for the following fiscal year. These do not affect payments; the profiles are used for projecting accruals and out of tolerance variances. This system is a read-only reporting system and does not collect data. It reports on data in the UPPS system. It displays master data that includes vendor identifiers and billing records.
- **Visual Invoice Tracking and Payment (VITAP)** - The Visual Invoice Tracking and Payment (VITAP) application is a front end accounts payable matching system that provides a variety of functionality for the Federal Acquisition Service (FAS) and Public Building Service business lines. VITAP provides data for two of the OCFO Web applications: Web Vendors and Invoice Search. It also provides interfaces for UPPS utility payment data to flow into Pegasys. External customers use Web Vendor to submit invoices via the web. Invoice hardcopies are scanned and entered into ImageNow. VITAP provides the interface between the FAS feeder systems (Online Management Information System (OMIS), Regional Business Application (RBA), and Telecommunications Order and Pricing System (TOPS)), document matching, validation, and processing, exception processing, workflow routing, invoice tracking, obligations processing, payment, accruals document management for unprocessed documents, transaction history, and Pegasys. VITAP automatically performs a match on the electronic and scanned documents and generates the appropriate accounting entries to be batched and transmitted to Pegasys. Some of the key functions that VITAP performs are invoice tracking, email notifications, report generation, and management information. VITAP uses the following information from a feed from Pegasys: Vendor Name, Tax Identification Number / Social Security Number, Address, email address. The vendor name and SSN only comes in as personal data where a vendor is a sole proprietor using their personal information for business purposes.
- **Web Vendor** - 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.

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?

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

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 from replacing an SSN entered by a vendors 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.

Individuals can decrease the potential risk to their privacy by obtaining and using an TIN instead of their SSN when doing business with the government. The SORN identifies that the vendor code is used for retrieval as well as the vendor's name.

This PIA will be posted to the GSA privacy site here - <https://www.gsa.gov/portal/content/102237> . The Pegasys SORN which covers this data will be replaced here - <https://www.federalregister.gov/documents/2013/12/31/2013-31308/privacy-act-of-1974-notice-of-an-updated-system-of-records> with updates to rename it and align with the information in this PIA.

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.

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.

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 however.

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.

This PIA will be posted to the GSA privacy site here -

<https://www.gsa.gov/portal/content/102237> . The Pegasys SORN which covers this data will be replaced here - <https://www.federalregister.gov/documents/2013/12/31/2013-31308/privacy-act-of-1974-notice-of-an-updated-system-of-records> with updates to rename it and align with the information in this PIA.

The following SORN captures the records discussed in this PIA:

<https://www.federalregister.gov/documents/2006/10/16/E6-17069/privacy-act-of-1974-notice-of-a-new-system-of-records>

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?

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 e-mail) 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? 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. FEDPAY also interfaces to Pegasys through the Secure Transfer Service. 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?

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? 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. Another example is VITAP's ability to generate accounting entries based on submitted documents.

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?

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.

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?

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 directly from the individual or is it taken from another source? If so, 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 e-mail address.

The data provided from ACA to Pegasys is not the personal data and is not shareable. For example, ACA (in VITAP) may create accounting lines in Pegasys against purchases in the system. This information is not shareable and does not contain personal data.

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?

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.

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 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 from replacing an SSN entered by a vendors 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.

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?

Users for all of the applications listed in this PIA, except for FEDPAY for vendors and Invoice Search, 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.

Invoice Search users are controlled through the USDA Pegasys account management process and roles are assigned in the Pegasys system by the USDA administrators.

FEDPAY for non-Government users are not approved through EARS but are approved by the vendor points of contact, i.e. the person appointed by each vendor to approve such requests.

The roles define whether the user has read-only or write privileges. The read/write privileges may change for different drawers in the system.

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

The Ancillary Corporate Applications (ACA) FISMA system was approved with an Authority to Operate (ATO) on September 21, 2016 and is in the process of being renewed. The system is a Moderate system and will be approved for three years on or before September 20, 2017.

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.

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?

Audit log reviews are performed when suspicious activity is detected or a security incident has been reported.

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.

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.

7.2 What procedures 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? If so, how?

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.

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.

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.

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 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.

OARS, CARS, and Check Cancellation are read-only applications and therefore do not have auditing enabled.

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.

^[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.