GSA Privacy Impact Assessment (PIA): PIA-458

Created Date: 1/30/2024 3:04 PM Last Updated: 8/16/2024 11:41 AM

General Services Administration

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.

PIA

General Information

PIA ID:	PIA-458	**PIA Status:**	Completed
System Name:	Pegasys		
Export PIA:	Yes		
CPO - Approval Date:	2/21/2024		
PIA Expiration Date:	2/20/2027		

Stakeholders Approvals

Information System Security Manager (ISSM) Approval

Name (Full)
Richard Banach

System Owner / Program Manager Approval

Name (Full)
Trena Ivy

Chief Privacy Officer (CPO) Approval

Name (Full)
Richard Speidel

PIA Overview

A.System Name:	A. System, Application, or Project Name:	Pegasys
B.Includes:	B. System, application, or project includes information about:	Pegasys, is a commercial-off-the-shelf financial system hosted in the CGI Federal Infrastructure as a Service (IaaS) Cloud and provides financial transaction processing and financial analysis for its main business lines of Federal supplies and technology, public buildings, and general management and administration offices. GSA also utilizes this system to operate a shared-services platform to provide financial management line of business (FMLOB) operations to external boards, commissions, and other federal agencies. The system information will be accessed and used by GSA employees and external clients. PFS serves as a comprehensive and integrated platform designed to manage, process, store, and disseminate financial information within GSA and Multitenant Shared Application (MSA) information system environments and plays a pivotal role in streamlining financial data-related processes and facilitating seamless communication across various government agencies/departments and external vendors. Pegasys users can create a purchase order, generate payments for credit card purchases, access/update budget and planning information, create estimate accruals/receipts to allow automated disbursements. Other processes such as FedEx and UPS send billing information to Pegasys for payment of services provided to customers. In addition, US Bank sends billing information to Pegasys for payment of credit card charges incurred by customer associates for official travel and expenses. These functions are performed by the Multitenant Shared Application for all external Customers. The data stored in PFS (GSA Pegasys and MSA) is financial accounting-related data. The Momentum product uses and stores the data in an Oracle

database. The data types include: General Ledger, Journals, Transactions, Payments, Fixed Assets, Vendors/Customers, Billing, Contracts Management, Project Cost Accounting, Travel Accounting, Credit Card, Leases.

For data in transit, HTTPS and TLS 1.2 are implemented. As for the input files that are transferred by sftp the PFS, a process described in the “Protection of PII” document is used to coordinate the encryption of fields sent from the feeder systems to PFS. The encryption algorithm is AES256. The feeder system encrypts the PII fields with the public key and transfers the file to PFS. When Momentum batch job is kicked off, the batch job script decrypts the input files using the private key. At no time is the data available unencrypted in the system. Every 90 days, the keys are reset through a process that is coordinated by GSA operations staff.

PFS collects, processes and stores the following sensitve personally identifiable information (PII);

ADDR - Relevant only to Employees
AGENCY ACCOUNT
BANK ACCOUNT NUMBER
CREDIT CARD HOLDER NAME
CREDIT CARD NUMBER
SSN

Additional text fields that are not business keys may also be configured as secured fields.

Agencies may specify how secured fields are presented to users without the ability to view the field. The presentation options include complete masking (i.e., displayed as asterisks), partial masking with a configurable number of characters viewable at the beginning of the secured field, and partial masking with a configurable number of characters viewable at the end of thesecured field.

Performing Searches Using Secured Data/Fields

When performing a search with a secured field entered as search criteria, the records returned will be limited to records with Security Organizations for which the user has view permission for the secured field.

If a search is performed with secured data and a Security Organization as search criteria, records having a matching Security Organization and secured data will only be returned if the user has view permission for the secured field in the given Security Organization.

C.Categories:	C. For the categories listed above, how many records are there for each?	The categories listed above have record counts that are constantly changing.
D.Data Elements:	D. System, application, or project includes these data elements:	The data elememts are sourced from GSA employees, other federal employees, contractors and members of the public and include the following; ADDR - Relevant only to Employees AGENCY ACCOUNT BANK ACCOUNT NUMBER CREDIT CARD HOLDER NAME CREDIT CARD NUMBER SSN
Overview:	Pegasys is a commercial off-the-shelf financial management system that was recently transferred from USDA ownership to GSA ownership on 2/26/2023. In the current PFS environment hosted in the CGI Federal Infrastructure as a Service (IaaS) Cloud, there are two separate instances of the Momentum application – Pegasys and a Multi-Tenant Shared Application Environment (MSA). GSA's instance of Momentum is Pegasys. The approximately 40 independent agencies, boards, and Presidential commissions are in the MSA instance. In both instances, PFS is uses a commercial off-the-shelf (COTS) version of CGI Federal's Momentum Financials™, which supports the processing of accounting transactions. Both Pegasys and MSA are the tools used to support PFS customers' financial reporting. GSA Pegasys and MSA do not communicate between each other. GSA application users access through their device using Secure Auth Multi Factor Authentication (MFA) through the VPN tunnel to PFS. The GSA Momentum/Central Contractor Registration Connector (CCRC) application. is load balanced and accessed via the established VPN tunnel to PFS. Application users of the Multitenant Shared Application (MSA); other than USIP, Ability One, and FEC, currently access the environment via a GSA owned and maintained Citrix platform. Once the user is authenticated to GSA's Citrix environment, the user is able to establish a connection to the MSA environment via a username/password authentication which traverses the GSA network through the VPN to the MSA Momentum/CCRC application. USIP, Ability One, and FEC application users access through their device using Login.gov MFA through the VPN tunnel to the Pegasys. There they will load balance to the MSA Momentum/CCRC application. CGI provides Tier 1 support. Administration of the CGI Federal IaaS is allowed for CGI Admins accessing via Federal Cloud SSL VPN The Cloud VPN includes profiles which limits users' access to only the zones the user is authorized to access. Customer access via two factor authentication through SSL VPN using Entrust IdentityGuard token. CGI Federal provides Tier 2 support for the PFS application. Administration of the PFS application is allowed for CGI Federal Admins accessing via CGI IPSEC VPN tunnel. The Federal Pulse VPN uses MFA and includes profiles which limits users' access to only the Pegasys.	

1.0 Purpose of Collection

PIA-1.1:	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?	Chief Financial Officers (CFO) Act of 1990 (Pub. L. 101-576) as amended. 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€“1.
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?	GSA/PPFM-11 (Pegasys) SORN applied to the information being collected.
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. Records are maintained in the system to allow for historical research and the possibility of further transactions processing. The Pegasys financial records are the system of record, but GSA currently maintains the Affordable Care Act (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. 1Explain:	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?	PFS collects information for purposes of financial planning and management, payment processing, reporting to government agencies, such as Treasury and the Office of Management and Budget for budget execution, cash disbursements, funds management (budget execution and purchasing), credit cards, accounts payable, disbursements, standard general ledger, reporting and other financial obligations.
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	Yes

PIA-3. 2Explained:	If so, how will this data be maintained and used?	Pegasys is designed to run as a web-based application and is supported by server equipment in CGI Federal's FedRAMP Cloud data center. User's government issued PCs are also required for data entry and connect through secured network lans and remote VPN access to these networks. Interfaces are accomplished via the translating of systems data to a standard record format required for the Pegasys system, i.e., the transformation box. Additionally, GSA utilizes the Financial Management Enterprise Service Bus (FMESB) for interfacing with Pegasys. Included under the Pegasys system umbrella is a data warehouse reporting database Financial Management Information System (FMIS). This system stores data from the Pegasys system for transactional processing and reporting purposes. Pegasys users can create a purchase order, generate payments for credit card purchases, access/update budget and planning information, create estimate accruals/receipts to allow automated disbursements. Other processes such as FedEx and UPS send billing information to Pegasys for payment of services provided to customers. In addition, US Bank sends billing information to Pegasys for payment of credit card charges incurred by customer associates for official travel and expenses. These functions are performed by the Multitenant Shared Application for all external Customers. Pegasys users can create a purchase order, generate payments for record credit card purchases, access/update budget and planning information, create estimated accruals/receipts to allow automated disbursements. Other processes such as FedEx and UPS send billing information to Pegasys for payment of services provided to customers. In addition, US Bank sends billing information to Pegasys for payment of credit card charges incurred by customer associates either for the government purchase card or for official travel and expenses. These functions are performed by the Multitenant Shared Application for all external Customers. In addition, Pegasys records accounts receivable transactions and generates billing to both Federal and on-federal customers. Upon receiving payment of the accounts receivable, Pegasys records the receipt of payment and liquidates the record. Please note these same comments apply to the PIA Overview (B))

PIA-3.3:	What protections exist to protect the consolidated data and prevent unauthorized access?	Access is limited to authorized individuals with passwords, and the database is maintained behind a certified firewall. Information on individuals is released only to authorized persons on a need-to-know basis and in accordance with the provisions of routine use. Additionally, vulnerability scanning, real-time intrusion detection, firewall monitoring and alert, active directory monitoring, database monitoring, site protection monitoring, identity management monitoring, monthly virus and compliance scans are performed on scheduled basis to ensure adequate security measire are in place to prevent unauthorized access.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3. 4Explain:	Please elaborate as needed.	Not applicable.
PIA-3.5:	What kinds of report(s) can be produced on individuals?	System does not monitor the public, GSA employees or contractors.
PIA-3.6:	Will the data included in any report(s) be de-identified?	Yes
PIA-3. 6Explain:	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-3.6Why 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?	Other Individuals Federal Agencies
PIA-4.2How:	If so, how will GSA share the information?	Pegasys financial and PII data is shared with the following organizations, for the purpose of accurate accounting transactions: Department of the Treasury, for monetary disbursements Internal Revenue Service, for tax reporting and collection. Grants data is shared with external grantees for the purpose of awarding and status. AbilityOne, FEC, USIP Defer to the SO and Gregg Rovinsky
PIA-4.3:	Is the information collected:	From Another Source
PIA-4.3Other Source:	What is the other source(s)?	AbilityOne, FEC, USIP
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes
PIA-4.4Who How:	If so, who and how?	CGIF Federal IaaS Cloud (FedRAMP ID: F1206061350) Central Managed Security Services (to include SIEM, AV, HIPS, etc.) GSA ISA FS/ESC - Unidirectional (PFS initiates). Payment, Ginvoicing, IPP from PFS to Treasury systems. FM/ESB - Data Incoming. Financial data from multiple GSA's source systems to GSA FM-ESB to PFS. GSA FM-ESB was established by GSA to streamline financial data exchange with PFS. SAP Concur - Unidirectional (PFS initiates). Travel data from PFS to Treasury systems
PIA-4. 4Formal Agreement:	Is a formal agreement(s) in place?	Yes
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	There are a series of edits built into the Pegasys application software that ensure information entered is valid and correct. These edits are checked in real-time as external and internal users input financial data into Pegasys for processing and when data are transmitted from systems that interface with Pegasys inputs that do not pass the Pegasys edit checks will not be allowed to proceed further and an online pop-up window will notify the user of the error or requirement for that field(s). Pegasys has built in integrity controls that validate that the appropriate data is entered into the application system by Pegasys users. There are a series of edits built into the Pegasys application software that ensure information entered is valid and correct. Some of the edits contained within Pegasys are as follows: spending edits; validity edits; relationship edits and tolerance edits.

6.0 Security

PIA-6.1a:	Who or what will have access to the data in the system, application, or project?	GSA Employees Contractors Members of the public Other Federal Employees SecureAuth, Encrypted VPN tunnels using RSA tokens, Single Sign On. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary.
PIA-6.1b:	What is the authorization process to gain access?	The preferred option to authenticate to Pegasys is to use Single Sign-on(SSO). Single Sign-on can be configured to authenticate with customer agencies' Identity Provider (IDP). Momentum is able to support SAML, Kerberos, X509, LDAP, and Active Directory. The choice is left to the customer agency. Once the IDP is determined and configured, the end user has to be authenticated by their agency's network before Pegasys allows them in through Single Sign-on. Other levels of access can be granted with supervisor approval or approval from a higher level authority. All access transactions, including approvals, additions, or removals of access are fully logged by the system.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	No
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	

PIA-6.3:	How will the system or application be secured from a physical, technical, and managerial perspective?	The GSA physical and environmental protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the physical and environmental protection for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site.
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?	PII incidents generally follow the same process and mitigation activities but include escalation within 1 hour to the IART as soon as potential PII is found to be at risk, in accordance with CISA guidelines. Details are in CIO 9297.2C CHGE 1. For Major Incidents involving PII, see Section 2.5.1. Incidents involving PII that are not "major incidents" generally follow the same process and mitigation activities but include escalation within 1 hour to the IART as soon as potential PII is found to be at risk, in accordance with CISA guidelines. PII incidents include, but are not limited to, the unintentional or intentional loss of information; or unauthorized access, acquisition, modification, or disclosure of PII information whether physical or electronic.

7.0 Individual Participation

PIA-7.1:	What opportunities do individuals have to consent or decline to provide information?	Individuals are given the opportunity and the right to decline provision, based upon protections and limitations in various U.S. Regulations, Acts, guidelines, policies, etc., at the myriad points of collection.
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7. 1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
PIA-7.2:	What are the procedures that allow individuals to access their information?	Individuals may obtain information regarding the procedures for gaining access to their own records contained within Pegasys by submitting a request to the Privacy Act Officer, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and all letters contained therein, should bear the words “Privacy Act Request.” A request for information should contain the name of the individual, the individual’s correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s).
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-7.3How:	How do individuals amend information about themselves?	Procedures for contesting records are the same as procedures for record access in section PIA-7.2 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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.	All GSA employees and contractors receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users are required to take additional, more detailed security training commensurate with their access permissions.

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?	The System Owner ensures the information is used only in accordance to the stated practices by reviewing audit logs, implementing role-based access control (RBAC), encryption of data. In addition, PFS undergoes an annual audit as well as user recertfication.