Privacy Impact Assessment

Pegasys

Technology, Planning, Architecture, & E

- Version: 1.3
- Date: February 3, 2020
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for

Pegasys

October 3, 2019

Contact Point
Gregg Rovinsky
Supervisory IT
Specialist
USDA ACFO-FMS
202-378-8962

Reviewing Official
Kenneth McDuffie
Information System Security Program Manager
USDA ACFO-FMS
504-426-5625

USDA OCFO

14th & Independence Ave SW, Washington, DC 20250

Abstract

This Privacy Impact Assessment (PIA) describes the collection, use, processing, and dissemination of personally identifiable information (PII) by the Pegasys system. Pegasys Financial Services (PFS) is part of the United States Department of Agriculture/Office of Chief Financial Officer (USDA/OCFO) and operates a financial management line of business that serves the needs of Federal government agencies. Pegasys and the Multitenant Shared Application provides financial management services to an excess of 40 independent agencies, boards, and commissions, including: all accounting functions related to accounts payable and accounts receivable; financial accounting treatment of acquiring and disposing of assets; and general accounting functions, such as performing/processing cost transfers, prior year recovery sampling/validation, Financial Management Services (FMS) 224 reporting, standard general ledger reconciliations, journal entries, accounting reports, and analysis of standard general ledger accounts. This PIA is required by the E-Government Act of 2002 since Pegasys processes, stores, and transmits PII data, as identified in the Privacy Threshold Analysis conducted for Pegasys.

Overview

System Name: Pegasys

USDA Component: Office of the Chief Financial Officer

Purpose: Pegasys and the Multitenant Shared Application contains sensitive financial information including credit card numbers, social security numbers, financial information of government employees and vendors/customers that do business with USDA. Pegasys processes and stores data for USDA and other USDA government customers. Pegasys contains PII information on government employees.

Description: The basic flow of end-user processing through the application front-end comprises the end-user traffic arriving at the Pegasys system over the client's corporate Wide Area Network. The application is accessed via a URL over HTTPS. Load-balancers direct incoming requests to Apache proxy servers in the DMZ. The Apache servers in turn direct the requests using round-robin architecture to the presentation tier running on Weblogic servers. For business processing, the Weblogic layer sends requests to the business tier that runs on C++ Tuxedo middleware. Data retrieval, updates and storage is performed in the database tier that utilizes Oracle RDBMS. Workflow request is handled by Webmethod BPM in Pegasys. For instance, if a document requires an approval before it can be processed, Webmethods BPM sends the approval request to the appropriate approver groups. The request will be sent to the approver's inbox within the application.

Pegasys Hosting maintains a separate Reporting database for GSA since their database is so large, in order to facilitate month-end reporting. SharePlex database software is used to replicate the data from PEGASYS into the REPORTS database where the data is extracted for reporting. For all other customers there is no separate reporting database established.

Batch jobs are run using Tivoli Workload Scheduler (TWS) that is managed by the operations team. Many of the jobs are kicked off automatically through TWS job streams and schedules. Batch jobs run as C++ programs in the Tuxedo layer. For those jobs that require input files from the client's systems, the files are transferred via sftp to the SFTP server in the DMZ. The files are

then moved automatically to the "infile" directory on the application servers; this directory is configured as the location where batch jobs can process input files. Some batch jobs result in output files or notification files that are placed in the outbound directory on the sFTP server. In some cases, the output files are sent via sftp by batch jobs to the client's designated server. For instance, GSA has an STS (Security Transfer Service) server where some outbound files are sent to by batch jobs.

Interfaces of customer agency clients to Pegasys arrive via flat files or web services. Flat files are sent to the sFTP server to be picked up by batch jobs. Web service calls are handled by the Weblogic layer that interacts with Tuxedo processes for business processing. For example, GSA mediates data from external systems via their Financial Management Enterprise Service Bus before sending to Pegasys. On the server side, there is a secure Shell service running all the time, but connections are done on a case by case basis. The Secure FTP process always requires authentication.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

USDA owns and operates PEGASYS, USDA does not use PEGASYS therefore no USDA employee PII is collected.

PII/Secured fields
The following fields are secured fields in Momentum:

* SSN/EIN
* (Vendor) Bank Account Number
* Agency Bank Account Number
* Alias Bank Account Name
* Bank Account Name
* Signatory Legal Name
* Signatory Company Name
* Vendor Name
* Credit Card Number
* Lock Box Number
* Sub-Bank Account Number
* Vendor DUNS
* Vendor DUNS+4
* Vendor Address Information (Address, City, State, Zip, County, Country, Phone, Fax, Email)

* Vendor Contact
* Database username and password
* Employee annual salary
* Employee hourly salary
* Pay scale grade
* Pay scale step

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 the secured 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.

1.2 What are the sources of the information in the system?

Based on GSA policy, since we are using the GSA network for now, some of these sources require ISA's and some of them don't. For a list of interfaces that require ISA's or MOU's please see the Pegasys Hosting System Security plan.

- Fedpay
- Vitap
- Transfer Box
- Pars Payroll
- US Bank
- Fedex
- United States Commission of Civil Rights (USCCR) – MSA
- Defense Facility Nuclear Safety Board (DFNSB) – MSA
- Federal Election Commission (FEC)
- FMESB
- UPS

- Treasury
- Concur

1.3 Why is the information being collected, used, disseminated, or maintained?

This data is used for financial planning and management, to make payments, and for reporting to government agencies, such as Treasury and the Office of Management and Budget for budget execution, cash disbursements, and other financial obligations.

1.4 How is the information collected?

Pegasys is designed to run as a web-based application and is supported by server equipment in CGI Federal's FISMA 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 storesdata from the Pegasys system for transactional processing and reporting purposes.

1.5 How will the information be checked for accuracy?

2 There are a series of edits built into the Pegasys application software that ensures 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.

2.1 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

- 5 U.S.C. Section 301, Departmental regulations.
- 5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence.
- 26 U.S.C. Section 6011, General requirement of return, statement, or list.
- 26 U.S.C Section 6109, Identifying Numbers.
- 31 U.S.C. 3711 through 3719, Claims of the United States Government.
- 31 U.S.C. Money and Finance; Chief Financial Officers Act of 1990.-

2.2 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks identified include unauthorized access to individual or group PII data, or aggregation of non-specific data that could be used for malicious intentions, for the purposes of fraud, extortion, loss of public trust, or other abuses. Security controls have been implemented to further protect PII data processed and stored within the system. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view information about others can do so. The following security controls are also utilized and continuously reviewed to ensure a high level of protection for the Pegasys system and associated data:

- Annual Vulnerability Assessments
- Real-time Intrusion Detection
- Firewall Monitoring and Alerting
- Active Directory Monitoring
- Database Monitoring
- Site Protection Monitoring
- Identity Management Monitoring
- Monthly Virus and Compliance Scans
- Active Host Virus Monitoring

All systems interacting with Pegasys are required to have appropriate security controls.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

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.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Active Directory, TACACS, ArcSight SIEM(Security Information and Event

Management Tool.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Not applicable. Pegasys does not use commercial or publicly available information.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

SecureAuth, Encrypted VPN tunnels using RSA tokens, Single Sign On, PIV Mandatory. 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.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Pegasys data is retained by ACFO-FS for at least 6 years and 3 months.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. Records are retained in accordance with NARA policies, USDA DR 3080-001, *Records Management*, USDA DR-3090, *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*, et al.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

ACFO-FS has determined that data retention periods and practices are adequate to safeguard PII while ensuring that mission critical data is available to support system restoration in the event of unplanned outages. Data retained in encrypted.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what

information is shared and for what purpose?

ACFO-SS/Pegasys owns the system but does not use the system, so no information is transmitted or disclosed to any internal organizations.

4.2 How is the information transmitted or disclosed?

ACFO-SS/Pegasys owns the system but does not use the system, so no information is transmitted or disclosed to any internal organizations.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

N/A

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

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.
- Office of Management and Budget, for USDA financial reporting.

Grants data is shared with external grantees for the purpose of awarding and status.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

External sharing of PII data is compatible with the original collection. Routine uses of the information is covered in SORN GSA/PPFM -11, Financial Systems. OCFO will retain this SORN until Pegasys is hosted on the USDA network.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared almost exclusively via electronic file transfer. Manual data sharing (CD, hardcopy, etc.) is permitted only in rare and special circumstances. All Pegasys interconnections are safeguarded through security measures defined within established Memorandum of Understanding and/or Interconnection Security Agreements. Security controls applied to system interconnections are regularly assessed to verify and validate that security protections are operating as intended.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There are no significant risks associated with the external sharing of PII data. All personnel accessing Pegasys PII data are cleared and trained annually on the proper handling and protection of PII data. 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. Encryption of PII data ensures the protection of this data.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

U.S. Government intention to collect PII data is declared the System of Record Notice made publicly available within the U.S. Federal Register, as well as in the Privacy Act, and at data collection points throughout the Federal government. Individuals who enter their own PII data are notified of their rights and protections under the Privacy Act before providing information via those collection points, which are outside the scope of control of USDA ACFO-FMS.

6.2 Do individuals have the opportunity and/or right to 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.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals consent to particular uses of the information at the time of provision.

Grievances involving consent and unauthorized use of the information can be addressed to the collecting Government agency, to agencies listed within applicable System of Record notices, or through other legal means.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided at the time of collection. The mechanism for notification may vary depending on the Government agency or commercial entity that manages the collection point. No data is collected by Pegasys itself. Individuals seeking mitigation action can contact the USDA Office of the Chief Financial Officer directly, or the Government agency or commercial entity that collected the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to 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).

7.2 What are the procedures for correcting inaccurate or erroneous information?

Procedures for contesting records are the same as procedures for record access in section 7.1 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.

7.3 How are individuals notified of the procedures for correcting their information?

Notification is provided in the system of records notice available in the Federal Register. Procedures for contesting records are the same as procedures for record access in section 7.1 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.

7.4 If no formal redress is provided, what alternatives are available to the individual?

If formal redress is not possible after contacting USDA in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited to, filing civil and/or criminal complaints.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records Notice posted in the U.S. Federal Register. Internal employees may also contact their respective Human Resources and/or Privacy Office representative for further assistance.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

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

8.2 Will Department contractors have access to the system?

Yes, there are USDA contractors that have access to Pegasys.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All USDA 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.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The system is currently going through Phase 1 concurrency review.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Pegasys logs all accesses to sensitive PII data. These logs are sent to the ArcSight SIEM solution that is configured to alert for indications of misuse. The Pegasys hosting environment provides real-time monitoring of networked connections and data flow. User accounts are re-authorized annually for continued need and applicability.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

ACFO-SS owns and operates the system but does not use the system. Customers can only see their information and the customer is expected to follow their security policy with regards to sharing data. Each user in Pegasys has a limited and specific set of roles. Each role is defined such that it only gives access to the data needed for that role. Therefore, the definition of the role prevents a user from misusing the data.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Pegasys is considered an ACFO-FMS Major Application and a Cloud-based system.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Pegasys does not use technology that would prompt an increase in concern regarding privacy protection. Pegasys components are commercial off-the-shelf products that all benefit from robust security configurations developed by both government and industry.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes. The Pegasys System Owner and the ISSPM have reviewed both OMB M-10-22 and M-10-23.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not applicable. Pegasys does not utilize any 3rd party websites.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not applicable

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not applicable

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not applicable

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not applicable

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not applicable

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either

internally or externally?

Not applicable

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not applicable

10.10 Does the system use web measurement and customization technology?

Not applicable

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

Not applicable

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not applicable

Responsible Officials

United States Department of Agriculture

14th & Independence Ave SW, Washington, DC 20250

Approval Signature

Agency Responsible Officials

GREGORY ROY
Digitally signed by GREGORY ROY
Date: 2020.02.10 15:11:06 -06'00'

Scott Roy
Information System Security Officer
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture

Agency Approval Signature

KENNETH MCDUFFIE
Digitally signed by KENNETH MCDUFFIE
Date: 2020.02.10 15:43:16 -06'00'

Kenneth McDuffie
Information System Security Program Manager
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture

System Owner Signature

STANLEY MCMICHAEL
Digitally signed by STANLEY MCMICHAEL
Date: 2020.02.14 12:42:24 -05'00'

Stanley McMichael
Information System Owner
Office of the Chief Financial Officer for Financial Management Systems
United States Department of Agriculture