Privacy Impact Assessment for the VA IT System called:

Invoice Payment Processing System (IPPS)

Financial Services Center (FSC)

Financial Operations Service (FOS)

Date PIA submitted for review:

1/26/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Deea Lacey	Deea.Lacey@va.gov	512-386-2246
Information System Security Officer (ISSO)	Rito-Anthony Brisbane	*Rito-Anthony.Brisbane@va.gov*	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-981-4871

Abstract

IPPS stands for Invoice Payment Processing System. This is a business rules engine which intakes commercial invoices and outputs a payment file. IPPS is designed to eliminate the obsolete legacy technology currently in place and use the Pegasystems Process Rules Process Commander (Version 7.x) to develop a unified invoice payment processing platform. The solution will include the functionality necessary to intake invoices from all available formats, perform advanced business rule processing, obtain payment certification or 3-way matching (invoice, purchase order, receiving report), and create payment files for export to the VA Financial Management System (FMS). The project is consistent with the Financial Services Center (FSC) mission of providing financial services to Department of Veterans Affairs (VA) and other government agencies. The FSC payment product line supports over 300 Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA) facilities throughout the United States. The solution will improve payment processing results for our existing VA customers and result in a more attractive product for potential adoption by other government agencies. Expected benefits include: 1. Net Reduction of product line costs beginning in 2013 2. Improvement in payment accuracy 3. "Best of Breed" payment processing technology that meets OMB/Treasury requirements 4. Potential for expansion of invoice processing product line to OGA 5. Knowledge transfer of PEGA application development methods to FSC staff 6. Creation of reusable project assets available from FSC BPM virtual asset repository.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Invoice Payment Processing System (IPPS) owned by the Financial Services Center (FSC) technically managed under the FSC Financial Technical Center Project Management Office (PMO).

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

Invoice Payment Processing System (IPPS) is designed to eliminate the obsolete legacy technology currently in place and use the Pega systems Process Rules Process Commander (Version 7.1.9) to develop a unified invoice payment processing platform.

C. Indicate the ownership or control of the IT system or project.

Financial Technical Center (FTC) PMO

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

We have a user base of 40k users. So, we do save 40k emails and user IDs.

E. A general description of the information in the IT system and the purpose for collecting this information.

The purpose of IPPS is to perform payment processing. Data is processed to make payments to vendors providing services to the Dept of Veterans Affairs. The FSC processes payment invoices for all VA stations and VISNs. IPPS is an invoice payment processing system. Any information located on the invoice for payment will be collected for processing.

Although IPPS does not store the following types of data, it can access it: name, SSN, address, bank account info, and telephone numbers. Information Required as Payment Documentation: Name of vendor, vendor code, supplier tax registration number, buyer tax registration number, supplier company registration number, delivery tax registration number, ship from tax registration number, Taxpayer Identifying Number (TIN), banking information, contact name, contact title, contact telephone number, contact email address, contact mailing address. Also see CFR 1315-9, Required Documentation.

With a Web portal and Electronic File Transfer data is received via electronic transmission from another system.

IPPS does not intentionally collect PII/PHI information from Veterans or their family members. However, some of our clienteles are veterans and /or family members of veterans. Data collected is the vendor data from the invoice or Purchase Orders submitted to the FSC for payment. PII/PHI data may exist on the invoice sent to the FSC by the vendor for payment; however, this information is not requested or required.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

Limited information is shared/received internally with ECB and VBA. It is shared/received through electronic transmission methods in accordance with VA Policy. The type of information shared/received is limited to name, Tax ID, business address, phone numbers, and vendor email addresses.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

N/A

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.
Budget and Accounting Act of 1950, General Accounting Office, Title 8, chapter 3.
System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VA.
http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

N/A

4. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

N/A

K. Whether the completion of this PIA could potentially result in technology changes

N/A

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number

☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

PII Mapping of Components (Servers/Database)

Invoice Payment Processing System (IPPS) consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Invoice Payment Processing System (IPPS) and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAFSCSQLFOS520	YES	YES	Name TXID Business Address Vendor Email	To validate vendors and make accurate payments	Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and

					encrypted transmission.
VAFSCMUL9500	YES	YES	Name TXID Business Address Vendor Email	To validate vendors and make accurate payments	Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information inside IPPS is not directly collected from individuals. Web portal and Electronic File Transfer; Received via electronic transmission from another system.

(Web portal) Data collected is the vendor data from the invoice or Purchase Orders submitted to the FSC for payment. The data collected by IPPS is stored within the VA enterprise infrastructure and subject to all VA security protocols. PII/PHI data may exist on the invoice sent to the FSC by the vendor for payment; however, this information is not requested or required. The database is on prem.

IPPS creates reports and uses the information located in VA daily downloaded tables from the Financial Management System (FMS) for business rule processing. These tables are Payment History, Obligation, Unpaid Voucher, and Vendor table.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

N/A

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

N/A

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Web portal and Electronic File Transfer; Received via electronic transmission from another system. IPPS does not intentionally collect PII/PHI information from Veterans or their family members. However, some of our clients are veterans and /or family members of veterans. Data collected is the vendor data from the invoice or Purchase Orders submitted to the FSC for payment. PII/PHI data may exist on the invoice sent to the FSC by the vendor for payment; however, this information is not requested or required.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

N/A

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The data that the vendor provides is bumped up against the aforementioned information in 1.2. If there is missing or incorrect data IPPS will place the invoice in an exception workbasket for a technician to perform an action. The action would be to either find/correct the data or return the invoice to the vendor for missing information that is required in the prompt payment act for payment processing.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The data that the vendor provides is bumped up against the aforementioned information in 1.2. If there is missing or incorrect data IPPS will place the invoice in an exception workbasket for a technician to perform an action. The action would be to either find/correct the data or return the invoice to the vendor for missing information that is required in the prompt payment act for payment processing.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Budget and Accounting Act of 1950, General Accounting Office, Title 8, chapter 3; Full SSN is used for payment and accounting purposes to index, and store pay affecting documents. Also required for IRS tax reporting. System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers For Payment-VA
http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:
Sensitive Personal Information may be released to unauthorized individuals

Mitigation:
• IPPS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• IPPS relies on information previously collected by the VA from the individuals.
• Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
• File access granted only to those with a valid need to know.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

Name: Used to identify entity billing. Example: FedEX, UPS, Dell AT&T etc…
Social Security Number: SSAN not required/requested, but sometimes provided anyway
Mailing Address: Vendor's info Zip Code: Vendor's info
Phone Number: Vendor's info
Email Address: Vendor's info
Vendor Invoice Information: The use of Vendor invoice information is to pay the vendor. See abstract definition.

The IPPS system includes the functionality necessary to intake invoices from all available formats, perform advanced business rule processing, obtain payment certification or 3-way matching (invoice, purchase order, receiving report), and create payment files for export to the VA Financial Management System (FMS). This system is consistent with the FSC mission of

providing financial services to VA and other government agencies. The FSC payment product line supports over 300 VHA, VBA, and NCA facilities throughout the United States. The IT system improved payment processing results for our existing VA customers and resulted in a more attractive product for potential adoption by other government agencies.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

The tables mentioned in 1.2 are used for system analysis. These tables can be used for financial reporting and used for OIG cases since the data downloaded is from VA's system of record FMS.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

System doesn't do this.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Encryption at rest and in transit.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

Masking of SSNs

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

All employees and contractors are required to participate in general and role-based privacy training annually, all appropriate administrative, technical and safeguards have been implemented to protect IPPS, data accessed and displayed by the system and users of the system and these controls are reviewed regularly.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

-- Access is determined through FSC Organizational Role.
-- Completed and supervisor approved VA Form 9957

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
-- Yes

2.4c Does access require manager approval?

-- Yes

2.4d Is access to the PII being monitored, tracked, or recorded?

-- Yes

2.4e Who is responsible for assuring safeguards for the PII?

-- Information System Security Officer (ISSO)

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Name
Social Security Number
Mailing Address
Zip Code
Phone Number
Email Address
Vendor Invoice Information
Vendor invoice information

IPPS is an invoice payment processing system. Any information located on the invoice for payment will be collected for processing. Although IPPS does not store the following types of data, it can access it: name, SSN, address, bank account info, and telephone numbers.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Information is retained 6 years, 3 months, and 1 day.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001 Governed by General Accounting Office Regulations which require retention for records created prior to July 2,1975: 10 years and 3 months after the period of the account; records created on and after July 2, 1975: 6 years and 3 months after the period of the account. Records are normally retired to Federal Record Centers within 1 or 2 years after payment and audit. Link to retention schedule: NARA Records Schedule

3.3b Please indicate each records retention schedule, series, and disposition authority.

All records are retained or 6 years, 3 months, and 1 day. The VA records management process is used to request the disposal of the records. If there is a business or legal use communicated the records will be maintained longer.

Each service has developed file plans identifying what records they are maintaining. Approved NARA GRS are identified, and specific retention guidelines are documented and followed IAW VA Handbook 6300.1, Records Management Procedures. NARA GRS 1.1 item #10 (Disposition Authority DAA-GRS-2013-0003-0001) https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf identified records be maintained for the specified retention period.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic records are retained if required (GRS Schedule 1.1, Item #10), and are destroyed IAW NARA disposition instructions. [Destroy after 6 years, 3 months, and 1 day after final payment or cancellation, but longer retention is authorized if required for business use.] Nightly job that removes data outside of retention period deletes / destroys metadata and image to re-use file storage. If there are paper records needed to be destroyed, they are placed into large, locked bins throughout the facility. They are destroyed each Friday by a contracted shredder company.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or

Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

We do not use PII data for all testing & training purposes, the only data that is being used is mock data. Since the data is made up, we do not risk PII data.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation:
• IPPS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

• We are also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions.
• File access granted only to those with a valid need to know Access to the records is restricted to VA Finance employees. These records are protected from outside access by Federal Protective Service

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Financial Service Center (FSC)	Electronic Data Interchange (EDI)	Name, Tax Identification (TIN or SSN), business address, phone numbers	Electronic transmission methods in accordance with VA

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
			policy. SFTP via VLTrader
Veterans Benefits Administration (VBA)	(PA&I) Performance Analysis & Integrity	Name, Tax Identification (TIN or SSN), business address, phone numbers	Electronic transmission methods in accordance with VA policy. SFTP via VLTrader
Financial Services Center	Financial Management System (FMS)	Name, Tax Identification (TIN or SSN), business address, phone numbers	SFTP via VLTrader
Financial Services Center	Integrated Financial and Acquisition Management System (iFAMS)	Name, Tax ID, business address, email address, phone numbers	SFTP via VLTrader

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The IPPS provides access to large amount of Vendor data which is necessary for the purpose of providing services to the VA and billing for those services. The compromise of this information would constitute a breach of confidence with the Vendors served by VA.

Mitigation: The source data used in IPPS already exists in the other systems, and the electronic transfers of information are secure. All access is done through secure internal VA networks. Only selected users have access to PHI data.

• IBM's Enterprise Content Management system (FileNet is the Financial Service Center's new electronic records management system. It adheres to information security requirements instituted by the VA Office of Information Technology (OIT).

• Both contractor and VA are required to take Privacy, HIPAA, and information security training annually.
• Information is shared in accordance with VA Handbook 6500
• File access granted only to those with a valid need to know

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***sharing (can be more than one)***	
None	None	None	None	None

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:
N/A

Mitigation:
N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Department of Veterans Affairs provides public notice that the information is being collected. This notice is provided in 2 ways:

1) System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA https://www.oprm.va.gov/privacy/systems_of_records.aspx
2) This Privacy Impact Assessment (PIA) also serves as notice of the IPPS system. As required by the eGovernment Act of 2002, Public Law 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

N/A

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The Department of Veterans Affairs provides public notice that the information is being collected. This notice is provided in 2 ways:

1) System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA https://www.oprm.va.gov/privacy/systems_of_records.aspx
2) This Privacy Impact Assessment (PIA) also serves as notice of the IPPS system. As required by the eGovernment Act of 2002, Public Law 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Mandatory; vendors will not be paid unless vendor information is obtained and used to process the payment. It is mandatory for vendors to comply with the Prompt Payment Act.

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

IPPS does not collect PII/PHI information from individuals, Veterans, or their family members. Nevertheless, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA Regional Office, a list of where can be found at: http://benefits.va.gov/benefits/offices.asp.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk:
Privacy information may be collected prior to providing the written notice

Mitigation:
Additional mitigation is provided by making the System of Record Notice (SORN) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1. MOU/ISA document provide a binding agreement and procedures to protect the data transferred.

• IPPS does not collect information directly from individuals, Veterans, or their families.

• Information is used only to process vendor payments.

• Payments will not be paid unless information is obtained and used to process the payment

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions**. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Record access procedures:

Individuals or authorized representatives seeking information regarding access to and contesting of records may write, call, or visit the VA office to which the invoice/voucher was submitted.

IPPS does not collect PII/PHI information directly from individuals. Nevertheless, individuals may access their information via FOIA and Privacy Act procedures.

Vendors submitting commercial invoices can access their information by calling our customer care center (877) 353-9791

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

Not exempt

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Contesting record procedures:

Individuals or authorized representatives seeking information regarding access to and contesting of records may write, call, or visit the VA office to which the invoice/voucher was submitted.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

These SORNs associated with the data available via the IPPS portal can be found on-line at: http://www.oprm.va.gov/privacy/systems_of_records.aspx. If the invoice has erroneous or incomplete information the then vendor will be notified of what is missing or incomplete via snail mail or email if we have that on file.
IPPS does not collect PII/PHI information directly from individuals. Nevertheless, Veterans can correct/update their information online via the VA's eBenefits website.
http://benefits.va.gov/benefits/offices.asp

These payment records are compiled from documentation from the vendor, contractor, and employee; Dun and Bradstreet (identifying numbers); and procurement and authorization documentation generated by the Veterans Administration.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans can correct/update their information online via the VA's eBenefits website. • http://benefits.va.gov/benefits/offices.asp• For DHS & HHS, there are no other formal redress systems in place.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:
Inaccurate data may be used to process payments

Mitigation:
The information in IPPS is obtained via the vendor sending in an invoice as previously stated. If there is erroneous or inaccurate information, the vendor may need to submit a corrected invoice. Any validation performed would merely be the Vendor personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data. See answer under 7.1 for the vendors outlet to call regarding their information.

Section 8. 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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

• Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics.
• Individuals must have a completed security investigation
• Once training and the security investigation are complete, a request is submitted for access…before access is granted; this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.
Site administrator(s) established at each VA location and grant access to the appropriate people. They can grant a read only access or certifying official access. When access is granted or removed 9957 security forms are generated.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

N/A

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

External providers have read-only access to claim and payment information. Internal VA users have access to claim and eligibility information based on varying roles within the applications.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

• Contractors will have access to the system and their contracts are reviewed on an annual basis.
• Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.
• Contractors must have a completed security investigation.
• Once training and the security investigation are complete, a request is submitted for access
• Before access is granted, this request must be approved by the government supervisor, Information Security Officer (ISO), and Office of Information & Technology (OIT).

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Privacy and Information Security Awareness and Rules of Behavior (TMS course # 10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored.

Other required Talent Management System courses monitored for compliance: VA 10203: Privacy and HIPAA Training VA 3812493: Annual Government Ethics

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 24 November 2022
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 26 July 2023
5. *The Authorization Termination Date:* 22 January 2023
6. *The Risk Review Completion Date:* 06 Sept 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH) Moderate*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

N/A

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Deea D. Lacey 293519

Digitally signed by Deea D. Lacey 293519
Date: 2023.02.01 15:50:56 -06'00'

Privacy Officer, Deea Lacey

RITO-ANTHONY BRISBANE

Digitally signed by RITO-ANTHONY BRISBANE
Date: 2023.02.02 10:05:38 -06'00'

Information Systems Security Officer, Rito-Anthony Brisbane

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2023.02.14 16:24:17 -06'00'

Information Systems Owner, Jonathan Lindow

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VA.

http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices