Privacy Impact Assessment for the VA IT System called:

Pega – Office of Acquisition and Logistics Ratification Tracking System (Pega – OAL RTS)

VA Office of Information & Technology

Finance Operations and Support

eMASS ID #2358

Date PIA submitted for review:

11/22/24

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Moya Hill	Moya.Hill@va.gov OITPrivacy@va.gov	202-704-9025
Information System Security Officer (ISSO)	Melvin Davis	Melvin.Davis3@va.gov	504-875-7280
Information System Owner	Kenton Ngo	Kenton.ngo@va.gov	303-439-6138

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

The OAL RTS (Office of Acquisition and Logistics Ratification Tracking System) is a case management application to track the ratification of contract breaches as part of a project for the Office of Acquisition and Logistics (OAL). After the contracting staff is made aware of the occurrence of an Unauthorized Commitment (UAC) of funds, they initiate a ratification case in the RTS application to capture the request for ratification and provide an analysis and recommendation for the case for ratification, which is submitted to a variety of approvers within the contracting organization. As a component of documenting the breach of contract that leads to any given ratification under review, the contracting officer is responsible for uploading a variety of supporting documentation related to each unique case for ratification in the RTS application.

This system implements a business workflow using the Pega BPM (Business Process Automation) and automates a previously manual paper-based system into a digital workflow that stores and tracks the documentation required in tracking such ratifications. Exceptions are identified in the workflow where any missing information at the case level can be rectified. This system is being migrated from an on-prem Pega solution to the Pega Government Cloud.

Overview

The overview is the most important section of the Privacy Impact Assessment (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. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Pega - OAL RTS (Office of Acquisition and Logistics Ratification Tracking System) is a case management application to track the ratification of contract breaches.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA Controlled / non-VA owned and operated.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The number of individuals whose information is stored will depend on the number of cases tracked and number of individuals associated with each case.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

The information being collected is the name and contact info for the VA contracting officer and supervisor, and initiator, as well as vendor name and vendor Point of Contact information. The purpose is to track the parties involved.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

The OAL RTS system integrates with IBM FileNet Enterprise Content Management (ECM) to store and retrieve ratification documents approved by contracting officers for Ratification review. Additionally, the RTS, integrated with FSC Online Form Submission (OFS), will use the VA Global Address List (GAL) and VA Email Account for user administration activities, including User provisioning and de-provisioning.

F. Are the modules/subsystems only applicable if information is shared?

Yes

G. Is the system operated in more than one site to include primary and secondary 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?

The system is operated in a single site.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

The authority for maintenance of the system is 31 U.S. Code 3512 - Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control.

I. What is the SORN?

Pega – OAL RTS is covered by the SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf.

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

This SORN is dated September 28, 2023 and does not required amendment, revision or approval.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

L. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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. It must also match the information provided in question 3.4 of the PTA.

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
- ☐ **Full** Social Security Number
- ☐ **Partial** 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[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements:

- Work Email
- Work Phone Number
- Work Address (City/State/Postal Code)
- Vendor/Company Name
- UEID (Unique Entity ID) Number
- Vendor Point of Contact POC Email

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- Vendor Phone Number
- Vendor Street Address
- Vendor City
- Vendor State
- Vendor Postal Code

1.2 List 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 is collected directly from the contracting officers, initiators, and vendors. Information is not collected from other sources, such as a commercial aggregator.

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.

Information is not collected from other sources, such as a commercial aggregator.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The Pega OAL RTS system is designed to perform analysis and create reports.

1.3 Methods of information collection
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?

Pega - OAL RTS extracts name and contact information using automation and internal application programming interfaces (APIs) from VA Email Account and Global Access Locator.

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

The information collected is not collected on a paper form and is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and 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 system relies on accurate information coming from VA Email Account and Global Access Locator (GAL) and is not checked for accuracy.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, the system does not check for accuracy by accessing a commercial aggregator.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

Updated authorities by which the data is collected are 31 U.S. Code 3512— Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Management Act (FISMA); Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control.

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment and Accounting Transactional Data-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf. This SORN is dated September 28, 2023, and does not require amendment, revision, or approval.

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.

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: There is a risk that if the data were accessed by an unauthorized individual or otherwise breached that personal or professional harm may result for the individuals affected.

Mitigation: Pega Cloud® uses data-at-rest encryption (DARE) in all Pega Cloud environments. "Data at rest" refers to any content that the cloud service saves on a hard drive. Encryption of data at rest is implemented for all sandbox and production environments. All client data stored in volumes, databases, and S3 buckets in a Pega Cloud environment are encrypted with 256-bit Amazon Web Services (AWS) encryption. The keys are rotated on a regular basis and are securely stored in Amazon Key Management Service (KMS). In addition, while SSNs will be used for locating applicable persons from the Master Veteran index, SSNs will not be relied upon for internal person identification. When visible to the end user, SSNs will be masked to show only last 4.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Contracting Officer's Name	Used to identify	Not used

Contracting Officer's Email	Used for communication	Not used
Contracting Officer Supervisor Name	Used to identify individuals	Not used
Contracting Officer Supervisor Email	Used for communication	Not used
Initiator Name	Used to identify individuals	Not used
Initiator Email	Used for communication	Not used
Initiator's Supervisor Name	Used to identify individuals	Not used
Initiator's Supervisor Email	Used for communication	Not used
Vendor/Company Name	Used to identify	Not used
UEID Number	Used to identify	Not used
Vendor POC Email	Used for communication	Not used
Vendor Phone Number	Used for communication	Not used
Vendor Street Address	Used for communication	Not used
Vendor City	Used for communication	Not used
Vendor State	Used for communication	Not used
Vendor Postal Code	Used for communication	Not used

2.2 Describe the types of tools 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 OAL RTS is a case management application to track the ratification of contract breaches. After the contracting staff is made aware of the occurrence of an Unauthorized Commitment (UAC) of funds, they initiate a ratification case to capture the request for ratification and provide an analysis and recommendation. The data created includes UAC initiator, UAC vendor, and contracting officer contact information as detailed in Table 2.1 and Table 3.1.

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.

The information created is not related to individuals or veterans. The information created is about Unauthorized Commitment of funds and whether those funds should be authorized.

2.3 How the information in the system is 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?

Pega Cloud® uses data-at-rest encryption (DARE) in all Pega Cloud environments. "Data at rest" refers to any content that the cloud service saves on a hard drive. Encryption of data at rest is implemented for all sandbox and production environments. All client data stored in volumes, databases, and S3 buckets in a Pega Cloud environment are encrypted with 256-bit Amazon Web Services (AWS) encryption. The keys are rotated on a regular basis and are securely stored in Amazon Key Management Service (KMS).

Application security in Pega is configured at three levels:

- Data in transit
- Data at rest
- Data at display

Data in transit is secured with transport-level encryption for browser-based sessions and authentication profiles for connectors and services.
Data at rest is secured with an encryption mechanism provided by the database vendors/providers. Pega supports encryption of individual database columns as well; Pega has in-built encryption capability to encrypt data using advanced encrypt standard.
Data at the display is secured by defining access control policies based on roles and attributes.

Pega Cloud for Government (PCFG) inherits controls from FedRAMP High controls.

Encryption Module	**FIPS 140-2 Certificate #**	**System Component(s)**
AWS Elastic Load Balancer (ELB)	# 4523	• Customer Stack HTTPS and Transport Layer Security (TLS) Connections • Predictive Diagnostic Cloud (PDC) Application HTTPS and TLS Connections
AWS Virtual Private Network (VPN)	# 4523	• Customer Stack VPN Connections
AWS Relational Database Service (RDS)	# 4523	• Customer Stack Databases • PDC Application Database
AWS Key Management Service (KMS)	# 4523	• Encryption Key Management
AWS Nitro Card Security Engine	# 3739	• Data in Transit
AWS S3 Buckets	# 4523	• Data at Rest
CheckPoint	# 4264	• Remote Access / VPN
Okta IDaaS Certificate	# 4370	• Authentication

Okta IDaaS Certificate	# 4370	• Digital Signatures/Hash
Secure Kernel Code Integrity-(Windows)	# 3096	• Operating System Configuration
Libgcrypt Cryptographic Module-(RedHat Linux)	# 3784	• Operating System Configuration

The PCFG system inherits the above encryption functionality and controls from the AWS IaaS. The AWS IaaS maintains a FedRAMP Authorized package providing statements describing AWS implemented encryption security controls. Please refer to the AWS FedRAMP Authorized package for details. All of the AWS services within PCFG use cryptographic keys provided by the AWS Key Management Service hardware security module (HSM) (Cryptographic Module Validation Program (CMVP) Certificate # 4523.) Recently, the AWS Application Load Balancer (ALB) uses a new certificate for FIPS 140-3 (CMVP Certificate #4631).

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Social security numbers will not be collected, processed, or retained by this system.

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

System users must be authenticated during login. Additionally, users must agree to the Privacy Information Security Agreement Rules of Behavior once a year which dictates how VA employees use/safeguard PII/PHI.

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?

All VA employees and contractors are required to go through privacy, information security and VA Rules of Behavior (ROB) training. This training ensures that the end users know how to properly handle PII. Beyond the training, the system is designed to secure the data. Access to PII is granted within the system, by System Administrators, enabling users to view, modify, add, or remove data based on user roles and responsibilities.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

All training is documented and tracked through VA TMS (https://www.tms.va.gov).

2.4c Does access require manager approval?

Yes, a Service NOW work ticket must be submitted by the user's Manager to access the system.

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

All access to the system is captured and can be retrieved or reviewed at a later date.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Any Veteran Affairs employee who is an authorized system user or administrator has the responsibility for assuring safeguards for PII.

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*

- Contracting Officer's Name
- Contracting Officer's Email
- Contracting Officer Supervisor Name
- Contracting Officer Supervisor Email
- Initiator Name
- Initiator Email
- Initiator's Supervisor Name
- Initiator's Supervisor Email
- Vendor/Company Name

- UEID Number
- Vendor POC Email
- Vendor Phone Number
- Vendor Street Address
- Vendor City
- Vendor State
- Vendor Postal Code

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

Records are retained and disposed of 10 years after the final action is taken, but longer retention is authorized if required for business use in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 1.2: Grant and Cooperative Agreement Records.

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.
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?

Yes, all records stored within Pega OAL RTS are indicated in the retention periods described in Question 3.2 reflect General Records Schedules (GRS) published by the National Archives Records Administration (NARA).

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

The records retention schedule, series and disposition authority are:
General Records Schedule 1.2: Grant and Cooperative Agreement Records.
https://www.archives.gov/files/records-mgmt/grs/grs01-2.pdf

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.

Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. "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.

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.

Development and testing environments do not allow the use of PII; therefore, the system does not use PII for research, testing, or training.

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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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: The risk to maintaining data within the system is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: The system 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.
- System access is only granted to authorized VA contractors and clinical staff.
- Electronic storage media used to store, process, or access records is disposed of in adherence with VA Directive 6500 (VA CYBERSECURITY PROGRAM).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Pega OAL RTS** consists of <**5**> key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Pega OAL RTS** 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 server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Pega OAL RTS	Yes	Yes	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email	Tracking of contract breach information	Enterprise Service Bus (ESB) API (application programming interface)

			• Initiator's Supervisor Name • Initiator's Supervisor Email • Vendor/Company Name • UEID Number • Vendor POC Email • Vendor Phone Number • Vendor Street Address • Vendor City • Vendor State • Vendor Postal Code		
IBM FileNet Enterprise Content Management (ECM)	Yes	Yes	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email • Vendor/Company Name • UEID Number • Vendor POC Email • Vendor Phone Number • Vendor Street Address • Vendor City • Vendor State • Vendor Postal Code	Tracking of contract breach information	Enterprise Service Bus (ESB) API (application programming interface)
OFS (FSC Online Form Submission)	Yes	Yes	• Contracting Officer's Name • Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email • Vendor/Company Name • UEID Number • Vendor POC Email • Vendor Phone Number • Vendor Street Address • Vendor City • Vendor State • Vendor Postal Code	Tracking of contract breach information	API
VA GAL (Global Address List)	Yes	Yes	• Contracting Officer's Name • Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email	Tracking of contract breach information	Simple Mail Transfer Protocol (SMTP)
VA Email Account	Yes	Yes	• Contracting Officer's Name • Contracting Officer's Email	Tracking of contract	Simple Mail Transfer

			• Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email	breach information	Protocol (SMTP)

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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***
IBM FileNet Enterprise Content Management (ECM)	Identification of and communication with individuals involved with the Unauthorized Commitment of Funds cases being tracked by the system	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email	Enterprise Service Bus (ESB) API

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*
		• Vendor/Company Name • UEID Number • Vendor POC Email • Vendor Phone Number • Vendor Street Address • Vendor City • Vendor State • Vendor Postal Code	
OFS (FSC Online Form Submission)	Identification of and communication with individuals involved with the Unauthorized Commitment of Funds cases being tracked by the system	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email • Vendor/Company Name • UEID Number • Vendor POC Email • Vendor Phone Number • Vendor Street Address • Vendor City • Vendor State • Vendor Postal Code	API
VA GAL (Global Address List)	Identification of and communication with individuals involved with the Unauthorized Commitment of Funds cases being tracked by the system	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name • Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email	Simple Mail Transfer Protocol (SMTP)
VA Email Account	Identification of and communication with individuals involved with the Unauthorized	• Contracting Officer's Name Contracting Officer's Email • Contracting Officer Supervisor Name	Simple Mail Transfer Protocol (SMTP)

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*
	Commitment of Funds cases being tracked by the system	• Contracting Officer Supervisor Email • Initiator Name • Initiator Email • Initiator's Supervisor Name • Initiator's Supervisor Email	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: Privacy Information may be released to unauthorized individuals.

Mitigation: The system 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. Additionally, information is shared in accordance with VA Handbook 6500.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: No data is shared externally.

Mitigation: No data is shared externally.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Notice is not provided because information is not collected directly from individuals. **Notice of Privacy Practice (NOPP)** VHA Directive 1605.04 IB 10-163p (va.gov).

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

6.1b If notice was not provided, explain why.

Notice is not provided because information is not collected directly from individuals.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice is not provided because information is not collected directly from individuals. **Notice of Privacy Practice (NOPP)** VHA Directive 1605.04 IB 10-163p (va.gov).

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

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.

Information is not collected directly from individuals. **Notice of Privacy Practice (NOPP)** VHA Directive 1605.04 IB 10-163p (va.gov).

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

6.3 Do individuals have the right to consent to particular 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.

Information is not collected directly from individuals. **Notice of Privacy Practice (NOPP)** VHA Directive 1605.04 IB 10-163p (va.gov).

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: Information is not collected from individuals, so insufficient notice risks do not exist.

Mitigation: Information is not collected from individuals, so insufficient notice risks do not exist.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Access to and use of national administrative databases are limited to those people whose official duties require such access. The VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA provides information security training via the Talent Management System (TMS) to all staff and instructs staff on the responsibility each person has for safeguarding data confidentially. Individuals may gain access to their own information by submitting a Freedom of Information Act (FOIA) request outlined on the http://www.va.gov/foia/ or http://www.vets.gov websites.

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)?

The system is not exempt from the access provisions of the Privacy Act.

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?

Pega - OAL RTS is a Privacy Act system. Hence, individuals may gain access to their own information by submitting a Freedom of Information Act (FOIA) request (https://department.va.gov/foia/).

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.

Individuals have the right to request an amendment (correction) to their information if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. Requests must be submitted in writing, specify the information that needs to be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains their information.

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.

Veterans are informed of the amendment process in the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains their information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Alternatively, Individuals seeking information regarding access to information contained in this system of records are encouraged to file a FOIA Request electronically at https://vapal.efoia-host.com/ .

However, individuals may mail or fax requests to: Department of Veterans Affairs, Freedom of Information Act Services (005R1C), 811 Vermont Avenue, NW, Washington, DC 20420, Fax: 202-632-7581.

Additional notice is provided through the SORNs listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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 also 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 and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail their Privacy Act or FOIA requests to:
Department of Veterans Affairs,
Claims Intake Center,
P.O. Box 4444, Janesville, WI 53547–4444,
DID: 608–373–6690

Any individuals who have questions about access to records may also call the VA Benefits Hotline: 1-800-327-1000.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The NOPP discusses the process for requesting an amendment to one's records. The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. **Notice of Privacy Practice (NOPP)** VHA Directive 1605.04 IB 10-163p (va.gov).

SORN 13VA047 / 88 FR 60269: Individuals Submitting Invoices – Vouchers for Payment-VA
https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

In accordance with the SORN noted above and locally established data security procedures, access to file information is controlled at two levels: the systems recognize authorized employees by a series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties.

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?

All system users are internal to the agency, and the system does not share any information externally. Therefore, other agencies will not have access to the system. In accordance with the SORN, access to and use of national patient databases are limited to those persons whose official duties require such access, and VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests.

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.

In accordance with the SORN noted above and locally established data security procedures, access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access. Server level access is granted to developers on an as needed basis by the Information Security Officer (ISO). The ISO has granted server access to a small set of trusted developers approved to work with and diagnose production issues. Additionally, employees are required to sign a computer access agreement acknowledging their understanding of confidentiality requirements. In addition, all employees receive annual privacy awareness and information security training. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

All contractors who will design, maintain or utilize the system have signed NDAs.

8.2a. Will VA contractors have access to the system and the PII?

Yes, contractors will have access to the system. Contractors will also be involved in the design, development, and maintenance of the system.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors will also be involved in the design, development, and maintenance of the system.

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.

General Training includes VA Privacy Rules of Behavior, Privacy awareness training, HIPPA and VA on-boarding enterprise-wide training.

Users must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

No A&A done. This FIPS199 Moderate-classified system's IOC date is 2/28/2025.

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. ***(Refer to question 1.8 of the PTA)***

PEGA-OAL RTS uses Pega Cloud for Government Software as a Service (SaaS) hosted on AWS Government Cloud. Pega Cloud for Government is FedRAMP authorized.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

There is an agreement in place between the VA and Pega Cloud Service Provider. (Contract # NNG15SD21B)

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.

Ancillary data is not collected by Pega.

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.

VA has full authority over data stored in Pega OAL RTS.

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).

RPA is not being utilized.

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**
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.

MOYA HILL Digitally signed by MOYA HILL
Date: 2024.12.11 14:06:17 -05'00'

Privacy Officer, Moya Hill

MELVIN DAVIS Digitally signed by MELVIN DAVIS
Date: 2024.12.16 14:43:11 -06'00'

Information Systems Security Officer, Melvin Davis

KENTON NGO Digitally signed by KENTON NGO
Date: 2024.12.16 14:22:20 -07'00'

Information Systems Owner, Kenton Ngo

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; screen shot of a website collection privacy notice).

Notice was not provided because information is not collected directly from individuals.

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)