Privacy Impact Assessment for the VA IT System called:

Pay Adjustment Transaction (PAT) – DCPS Data Exchange (DDE) Cloud

Financial Services Center (FSC) Veterans Administration (VA)/VACO

Date PIA submitted for review:

June 16, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Princess Miller	Princess.Miller@va.gov	*512-460-5148*
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

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Pay Adjustment Transactions project will replace the Separated Employee Retirement (SER) function of the mainframe system to be decommissioned with a web based Pega solution. The Financial Payroll Services Payroll Stations will see little difference between the current system and the replacement solution.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Defense Civilian Pay System (DCPS) Data Exchange (DDE) application under the Pay Adjustment Transactions (PAT) project is developed to replace and improve upon the Separated Employee Retirement (SER) pay adjustment process currently handled in the soon to be decommissioned On-Line Data Entry (OLDE)The following shall be the new business process steps to facilitate the SER: 1. Employee Payroll update 2. Notification and Secondary Review 3. Notification and Final Approval 4. Formatted output files per Human Resource & Payroll Application Service (HR PAS) requirements for Financial Management System (FMS). Using PEGA technology, rebrand the portion of the Personnel and Accounting Integrated Data (PAID) On-Line Data Entry (OLDE) application that performs the Separated

Employee Retirement (aka Employee Retirement Corrections) pay adjustment transactions so that the VA will be able to decommission the OLDE system per the sunset date.

The VA employee's information is used to come up with the adjusted retirement corrections (pay and Retirement accounts), which are then transmitted to FMS, so that the employee's/ retiree's station suspense accounts in FMS are debited and credited as needed

The completion of this PIA is a result of the migration to VAEC cloud. PAT-DDE will use the VAEC Cloud Service Provider (CSP) Microsoft Azure GovCloud (MAG), which is FEDRAMP approved. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], VAEC Azure Government High Assessing was granted an ATO to be in effect for 120 calendar days on February 15, 2018. Security and privacy data held by a cloud provider is still required to meet the requirements under the privacy act. Federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" FedRAMP Policy Memorandum. The contract outlines Management of Security and Privacy Incidents IAW VA Handbook 6500.2. Based on determinations of independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages for affected individuals to cover the cost of providing credit protection services to affected individuals. CSPs are required to meet the same requirements when operating on behalf of the federal government.

Legal authority to operate: Budget and Accounting Act of 1950; General Accounting Office Title 8, Chapter #3; Authorized under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules.

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 Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

- **VA EIN**
- **HRSMART ID**

Add Additional Information Collected but Not Listed Above Here

PII Mapping of Components

PAT-DDE consists of several key components 2. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII used by **PAT-DDE** and the functions that are coming from Health Resources Priority and Allocations System (HRPAS) are mapped below.

PII Mapped to Components

PII Mapped to Components

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
HRPAS_AWS	Yes	Yes	Employee Name SSN VA EIN HRSMART ID DOB	Business processing and payments to VA employees	Access control, PIV authentication, Two-factor authorization, configuration management, etc. Due to the sensitivity of this information system, all personnel with System Administration rights and roles will require an elevated background investigation to fulfill their duties.
FSC	Yes	Yes	Employee Name SSN VA EIN HRSMART ID DOB	Business processing and payments to VA employees	Access control, PIV authentication, Two-factor authorization, Configuration management, etc. Due to the sensitivity of this information system, all personnel with System Administration rights and roles will require an

					elevated background investigation to fulfill their duties.

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

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

PAT-DDE is not a source of veteran data, HRPAS will have all the data elements which are used with in the SER application.

1.3 How is the information collected?

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?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

PAT-DDE does not collect any information. Data residing in the PAT-DDE is obtained from HRPAS.
User traits are received via REST service call through the Identity and Access Management (IAM) framework layer. IAM service is an authentication service specifically designed for controlling access for Department of Veterans Affairs (VA) internal users (employees and contractors) accessing VA applications. Report data is received from databases by database queries.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The PAT-DDE is not the original source of the information, rather it stores the data. There is no contract requiring data to be checked for accuracy on the PAT-DDE.

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

PAT-DDE does not collect any information. Data residing in the PAT-DDE is obtained from HRPAS

Legal authority: Budget and Accounting Act of 1950; General Accounting Office Title 8, Chapter #3; Authorized under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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: 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:
The Separated Employee Retirement (SER) application system has Social Security Number (SSN), Employee Name (EE Name), Date of Birth (DOB) and Veterans Administration Employee Identification data, which exposes it to possible compromise.

Mitigation:
The SER application system requires two-factor authentication to allow login in, meaning that the User must utilize their Personal Identity Verification (PIV) card to access the application. Only Veterans Administration (VA) full time employees can view employee data in the system. Contractors or other VA employees cannot login.

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.

The following data elements reside in the PAT-DDE application system.

- Emp Name: Emp Name is used identify the Employee Name with the user spreadsheet
- Emp ID: Employee ID is identified to use the identify Veteran
- Social Security Number: SSN is Used to identify the Veteran details
- VA EIN/ HRSMART ID: HRSmart id is used to identify the Veteran in HRPAS system
- Date of Birth: DOB is identified to use Veteran and confirm patient identity
- Year: Year is Used to identify the current year
- Day number: Day number is Used to identify the veteran deceased day number of that year
- Normal hours: Normal hours are Used to identify normal working hours.
- Pay Basis: Pay Basis is Used to identify veteran Pay grade details
- Duty Basis: Duty Basis is Used to identify Duty basis detail from HRPAS
- Pay Plan: Pay plan is Used to identify veteran pay plan
- Appointment Type: Appointment Type is Used to identify station type character
- FTE Equivalent: FTE Equivalent is Used to identify veteran data set
- Cost Center: Cost Center is Used to identify 6-digit number which belongs to station
- Sub Account: Sub Account is Used to identify duty station which is extension of station
- Fund Control Number: Fund Control Number is Used to identify veteran control number which is a combination of Station and Cost Center
- Labor Code: Labor Code is Used to identify veteran Pay Category
- Separation Year: Separation Year is Used to identify the veteran deceased year
- Separation Day Number: Separation Day Number is Used to identify the veteran deceased day number of that year
- Current Tax Year: Current Tax Year is Used to identify current Fiscal Year
- Amount: Amount is Used to identify the adjusted amount in decimal number

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

PAT-DDE identifies Separated Employees using a Social Security Number (SSN) search obtained from HRPAS and adjusts the Separated Employee payments. The adjustment contains the hours and the amount to be paid for the Separated Employee.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

The Separated Employee Retirement (SER) users are Access to PII is limited by role assignment, which is completed based on user role. Roles are assigned via SSOi and IAM provisioning process, where roles can be provided and loaded into the system for 104 station.
.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

<u>Principle of Use Limitation:</u> 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.

Add answer here:
The PAT-DDE Separated Employee Retirement (SER) application system has user authentication through SSOi (Single Sign On Internal) with IAM for the internal site. Access to PII is being monitored and logged. Responsibility for PII safeguards lies with the VA.

System of Records Notice (SORN) is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers For Payment-VA
https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf

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

The following data elements reside on the PAT-DDE for purposes of, but not limited to, making payments to separated VA employees.

- Emp Name
- Social Security Number/ VA EIN
- Date of Birth
- Year
- Day number
- Normal hours
- Pay Basis
- Duty Basis
- Pay Plan
- Type Appointment
- FTE Equivalent
- Cost Center
- Sub Account
- Fund Control Number
- Labor code
- Separation Year
- Separation Day Number
- Current Tax Year

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?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

User access form (9957) data is retained for 7 years as required by General Record Schedule (GRS) 6.1: Accountable Officers' Accounts Records for each claim as they are recorded separately. https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.

Yes, 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: 7 years after the period of the account; records created on and after July 2, 1975: Link to retention schedule: https://www.archives.gov/records-mgmt/grs

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

PAT-DDE follows guidelines required by General Record Schedule (GRS) 6.1: Accountable Officers' Accounts Records for each claim as they are recorded separately. https://www.archives.gov/records-mgmt/grs The data in the form that requires compliance with the General Record Schedule (GRS) 6.1 does not contain SPI. 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 comp

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

The VA Financial Services Center uses techniques to minimize the risk to privacy by disallowing the use of PII for research/testing/training. Our Information System Security Officer (ISSO) enforces the policy that the only environments that can have live data is production environment. Per VA Handbook 6500, security control SA-11: Developer Security Testing states: (c) Systems under development should not process "live data" or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

Sensitive Personal Information of SSN, Employee ID and Name may be released to unauthorized individuals.

Mitigation:

PAT-DDE adheres to information security requirements instituted by the VA Office of Information Technology (OIT).

- All the user access management tasks will be handled by IAM Provisioning.
- Both contractors 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 the 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***
Human Resources – Payroll Application Services (HR-PAS) Pay Adjustment Transactions – Defense Civilian Pay System Data Exchange (PAT-DDE)	Modernize the Veterans Affairs human resource and payroll reporting to VA stakeholders	1. VA Employee Name 2. VA Employee SSN 3. VA Employee DOB	JDBC with in Pega (Database to Database Link (use of views)
Financial Management System (FMS)	Adjusted retirement corrections (pay and Retirement accounts), which are then transmitted to FMS, so that the employee's/ retiree's station suspense accounts in FMS are debited and credited	• Employee ID • Day Telephone Number • Employee Name • Sub Account • Fund Control Number • Date of Birth • Separation Year • Separation Day Number • Current Tax Year	VL-Trader
Integrated Financial Acquisition Management System (iFAMS)	OnLine Transactional Process (OLTP) Production Database, Golden Gate Production Database, and Production Standby Databases have been included as connection.	• Employee ID • Day Telephone Number • Employee Name • Sub Account • Fund Control Number • Date of Birth • Separation Year • Separation Day Number • Current Tax Year	VL-Trader

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.
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:

- PAT-DDE 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.
- Information is shared in accordance with VA Handbook 6500
- Database access granted only to those with a valid need to know
- All access requests are logged and recorded.
- FSC Data Depot is an encrypted database inside the VA network
- Monitoring tools such as QRadar, Imperva are in place

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 office or IT system***	***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 sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

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:
PII such as SSN, Veteran name, date of birth and HRSmart id or employee id may be accidently released to unauthorized individuals.

Mitigation:
Information is only accessible to authorized individuals who gain access with their approved SSOi-provided with PIV card authentication. All users must take HIPAA and VA privacy and security training. Audit logs are in place.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

PAT-DDE application will use the source data from HRPAS Data center. Application user will not collect information from individuals.

13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data - VA

(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

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

PAT-DDE does not collect information from individuals; however, the information is collected from HRPAS which individuals can decline to provide information, and if so, will not be able to complete human resources and payroll activities necessary for employment.

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

PAT-DDE does not collect information directly from individuals; however, the information is collected from HRPAS which the use of PII within the PIA is not subject to consent. Data is collected for human resources and payroll purposes.

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.

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:

PAT-DDE does not collect information directly from individuals; however, the information is collected from HRPAS which provide notices to the individuals. There is a risk that individuals will not know that HR-PAS collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation:

PAT-DDE mitigates this risk by ensuring we provide an individual's notice of information collection and notice of the system's existence through the methods discussed in question 6.1

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The PAT-DDE system does not collect PII/PHI information directly from individuals. Nevertheless, individuals may always access their information via Freedom of Information Act (FOIA) and Privacy Act procedures.
VA employees may access their information by contacting their servicing HR office. Additionally, any Veteran may request access to one's own health documents by completing VA Form 10-5345a, (Individuals' Request for a Copy of their Own Health Information) which can be obtained online at https://www.va.gov/find-forms/?q=Form+10-5345a

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.

The PAT-DDE system does not collect PII/PHI information directly from individuals. Nevertheless, individuals may always access their information via Freedom of Information Act (FOIA) and Privacy Act procedures. VA employees may access their information by contacting their servicing HR office.

Additionally, any Veteran may request access to one's own health documents by completing VA Form 10-5345a, (Individuals' Request for a Copy of their Own Health Information) which can be obtained online at https://www.va.gov/find-forms/?q=Form+10-5345a

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.

PAT-DDE is not a source of data. All the data corrections will be handled at station level that is external to PAT-DDE. FTG stores and transmits data. Individuals wishing to correct their medical information would follow Veterans Health Administration (VHA) processes/procedures as VHA maintains the system of record.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

PAT-DDE is not a source of data. All the data corrections will be handled at station level that is external to PAT-DDE.The FTG stores and transmits data but does not process or correct it. Nevertheless, Veterans can correct/update their information online via the VA's eBenefits website: https://www.ebenefits.va.gov
VA employees may access/correct their information by contacting their servicing HR office. Additionally, the Privacy Officer provides appeal rights to the Office of General Counsel or VHA Privacy Office via the written response to the individual regarding the outcome of the amendment request.

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.

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:
There is a risk that individuals whose records contain incorrect information may not receive timely correspondence or services from the facility, e.g. incorrect information in a request for travel reimbursement could result in inability to generate proper payment.

Mitigation:

FSC FTG mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in Question 1.5. Additionally, FSC FTG's staff identifies incorrect information in individual records during payment transaction processing. Staff are also informed of the importance of maintaining compliance with VA Release of Information (ROI) policies and procedures and about the importance of remaining alert to information correction requests.

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

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

IAM service is an authentication service specifically designed for controlling access for Department of Veterans Affairs (VA) internal users (employees and contractors) accessing VA applications. PAT-DDE has user authentication thru SSOi (Single Sign On Internal) integration with IAM for internal site. Standard Operating Procedures (SOP's) are documented in the PAT-DDE User Guide.

PAT-DDE integrated with IAM Provisioning service to perform user access management. All Individual related access requests (Activation/Deactivation) are performed through IAM provisioning portal. User submits their access request in IAM and once the DDE approver approves the user access request in IAM then user will now have access to PAT-DDE.

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 not have access to PAT-DDE system. Contracts do not have HRSMART ID associated with them. So, only VA employees can have access to PAT-DDE.

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 (Talent Management System 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?

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

PAT DDE is minor application under FTG ATO which is approved until May 12, 2023. The system classification is Moderate.

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

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).

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.

PAT-DDE Cloud service provider, Microsoft Azure Government Cloud (VAEC MAG Cloud) under FEDRAMP moderate.

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)

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.

PRINCESS MILLER

Digitally signed by PRINCESS MILLER
Date: 2022.08.10 09:21:39 -05'00'

Privacy Officer, Princess Miller

RITO-ANTHONY BRISBANE

Digitally signed by RITO-ANTHONY BRISBANE
Date: 2022.08.09 17:57:32 -05'00'

Information Systems Security Officer, Rito-Anthony Brisbane

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2022.08.09 15:38:19 -05'00'

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).

(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data - VA