Privacy Impact Assessment for the VA IT System called:

Human Resources - Payroll Application Services (HR-PAS)

Technology Center (AITC) EMPO Austin Information

Date PIA submitted for review:

December 27, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Forte	Kimberly.forte@va.gov	202-461-5354
Information Security Officer	Andre Davis	Andre.davis2@va.gov	512-326-7422
System Owner	Dominique Banks	Dominique.Banks@va.gov	202-632-8602

Abstract

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

Human Resources - Payroll Application Services (HR-PAS) is the VA-wide system that collects payroll data, other Human Resources, and related fiscal operations for the VA data for reporting purposes.

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?*

HR-PAS is the VA-wide system that reports data received from the HR source system (HRSMART) and payroll source system (DCPS). The HR-PAS is a cloud-based application intended to modernize the Veterans Affairs human resource and payroll reporting to VA stakeholders. The HR-PAS application is located within the VA Enterprise Cloud Service (VAEC) enclave and the cloud service provider is Amazon Web Services (AWS) GovCloud located in Arlington, Virginia. Based on a

security risk assessment on the manner of VA data surrounding confidentiality, integrity, and access, HR-PAS is a moderate impact system. AWS however, is certified FedRAMP High. AWS GovCloud has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for high impact level. HR-PAS system of records comprises of personnel and payroll data across the VA enterprise nationwide and consist of records for over 575,000, active and separated, VA employees. All other access is limited to VA employees/contractors with desktop access from within the VA firewalls or secure access through IBM's Host on Demand internet software.

The following is a full list of related laws, regulations and policies and the legal authorities:

1. 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs 32 CFR
2. Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons
3. Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
4. 38 U.S.C. Chapter 74 – Veterans Health Administration—Personnel
5. Information from the SORN: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
6. 5 U.S.C. 552, "Freedom of Information Act," c. 1967
7. 5 U.S.C. 552a, "Privacy Act," c. 1974
8. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
9. Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
10. Federal Information Security Management Act (FISMA) of 2002
11. OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
12. VA Directive and Handbook 6502, Privacy Program

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
- ☐ Other Unique Identifying Information (list below)

Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)

Performance Codes and Review Rating, Disabled Veteran Leave, Birth Country Code, Citizenship Code, HCP Code, Sex, Type of Visa, Veteran Preference, VISA Country Code, Primary and Secondary State, Tax Marital Status, Federal Income Tax, Marital Status, City Tax Info, Primary and Secondary State Geographic Code, Primary and Secondary State Residence, Primary and Secondary State Tax, Additional Withholding, Primary and Secondary State Tax Exemptions.

PII Mapping of Components

HR-PAS consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by and the functions that collect it are mapped below.

.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

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
HR-PAS Production Database (PRODOLTP)	Yes	Yes	Social Security Number (SSN), Resident Address, Disability Retirement Indicator, Performance Code, Performance Review Rating, Disabled Veteran Leave, Birth Country Code, Citizenship Code, Date of Birth, HCP Code, Race & National Origin Code, Sex, Type of Visa, Veteran Preference, VISA Country Code, Primary and Secondary State, Tax Marital Status, Federal Income Tax, Marital Status, City Tax Info, Primary and Secondary State Geographic Code, Primary and Secondary State Residence, Primary and Secondary State Tax, Additional Withholding, Primary and Secondary State Tax Exemptions	Payroll and Human Resources data processing and benefit disbursement.	Secured method of data transfer through Secure File Transfer Protocol (SFTP)

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.

HR-PAS collects, and reports data received from DCPS, VATAS and HRSMART/Human Resources Information System (HRIS) Department of Veterans Affairs system of record for human resource data.

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 technology 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.

Data is collected via electronic transmission from HRSMART, VATAS, and DCPS.

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.

Accuracy of information is validated through functional specification testing to validate data values and mappings. Functional scenario-based testing includes both positive and negative testing, and file comparisons during parallel data entry and payroll phases.

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

The following is a full list of related laws, regulations and policies and the legal authorities:

1. 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs 32 CFR
2. Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons
3. 38 U.S.C. Chapter 74 – Veterans Health Administration—Personnel
4. Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
5. Information from the SORN: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
6. 5 U.S.C. 552, "Freedom of Information Act," c. 1967
7. 5 U.S.C. 552a, "Privacy Act," c. 1974
8. OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
9. Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
10. Federal Information Security Management Act (FISMA) of 2002
11. OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
12. VA Directive and Handbook 6502, Privacy Program

HR-PAS is a department-wide system that encompasses personnel, payroll, and related fiscal operations. The system is affected by the Office of Personnel Management (OPM) mandates; Federal and state legislation; executive orders; Office of Management and Budget (OMB) directives; and regulations of the Treasury Department, Internal Revenue Service (IRS), and Social Security Administration (SSA).

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk:
Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:
The HR-PAS team has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. HRIS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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.

Bi-weekly, quarterly and annual reports are generated for HR, payroll and financial services. These reports are stored on a mainframe system and AWS s3 buckets within the VA firewall and are accessible only to users with approved credentials.

1. **Name**: Used to identify the employee and retained for employee HR record
2. **Social Security Number**: Used as a unique employee identifier and retained for employee HR record
3. **Date of Birth**: Used to identify employee age and retained for employee HR record
4. **Mailing Address**: Used for communication and retained for employee HR record
5. **Zip Code**: Used for communication and retained for employee HR record
6. **Phone Number(s)**: Used for communication and retained for employee HR record
7. **Email Address**: Used for communication and retained for employee HR record
8. **Financial Account Information**: Used to support payroll direct deposit
9. **Beneficiary Numbers**: Retained for employee HR record
10. **Race/Ethnicity**: Voluntarily self-reported for employee HR record
11. **Compensation data**: Used to support payroll and compensation function
12. **Benefits information**: Used to provide employee benefits

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

The system does not perform analytical tasks that would result in the creation of newly derived data or new employee records.

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?

Data at rest and data in transit are encrypted.

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

All Data including PII at rest and data in transit are encrypted. No special protection for SSN and other PII.

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

All Data in use, at rest, and in transit including PII/PHI are encrypted.

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. 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.

In accordance with Austin Information Technology Center (AITC) guidance, AITC personnel that will be accessing information systems 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 VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. The minimum-security requirements for HR-PAS's moderate impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.

The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how personal information is used, stored, and protected.

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

All employee information that is collected and stored in the system, as identified in question 1.1, is retained by the system.

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.

Data will be retained in the HR-PAS Online Transaction Processing (OLTP) Database for all active VA employees and separated employees for 39 pay periods after separation. In addition, bi-weekly payroll data (plus employee snapshots) is retained for a minimum of 20 years.

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.

The disposition authority is documented in Record Control Schedule 10-1. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version-2/VA Policy, VA Form 0751, and Information Technology Equipment Sanitization Certificate. HR-PAS complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. HRIS records are retained according to Record Control Schedule 10-1.

No records are disposed of or destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

https://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf (Records Control Schedule 10-1)
www.va.gov/vapubs/viewPublication.asp?Pub_ID=20&FType=2 (VA Handbook 6300)
https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassificationmanual.pdf (NCSC-TG-025 Version-2/VA Policy)
http://vaww.va.gov/vaforms/va/pdf/VA0751(ES).pdf (VA Form 0751)

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

Under the jurisdiction of VHA, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 101. The GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records

Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.

Paper documents may be shredded or burned, and record destruction is documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG-025 Version-2/VA Policy. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version- 2/VA Policy, VA Form 0751, and Information Technology Equipment Sanitization Certificate.

No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

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

HR-PAS (the organization) develops policies, that minimize the use of PII for testing, training or research.

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:

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

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

Follow the format below:
Privacy Risk:
There is a risk that the information maintained by HR-PAS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation:
To mitigate the risk posed by information retention, the HR-PAS system adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the data will be carefully disposed of by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information and Technology	Integrated Benefits System (IBS) (HRPASIBS47)	Social Security Number, Date of Birth	File is put on mainframe for IBS team.
Board of Veterans Appeals	Veterans Appeals Control and Locator System (HRPASBVA16C)	Social Security Number, Date of Birth	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
Veterans Benefit Administration	Enterprise Data Warehouse (HRPASBVA16A) AVBA-RVBA	Social Security Number, Date of Birth, Sex, Veteran Preference, Race & National Origin Code, Birth Country Code, Performance Code, Performance Review Rating	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
VHA Support Service Center	Veterans' Health Administration (HRPASBVA16D)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Financial Services Center	Treasury Reconciliation - TSP Loss and Breakage (HRPASFSC56/HRPASFSC57)	Social Security Number	Bi-directional process using secure AWS S3 bucket
Financial Services Center (FSC)	Debt Management Center (HRPASDMC52)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
Financial Services Center (FSC)	Caregiver Support Program (HRPASFSC37)	Social Security Number	Bi-directional process using secure AWS S3 bucket
Financial Services Center (FSC)	DCPS Data Exchange FSC-PCS Exp API	Social Security Number	Application Programming Interface (API)
Financial Services Center (FSC)	Financial Management Business Transformation	Social Security Number, Sex, Veterans Preference, City Tax Deduction	Application Programming Interface (API)
Office of Information & Technology (OI&T) / Information & Technology Budget & Finance	IT Budget & Finance Database ITRM-DCBI Experience API	Resident Address	Application Programming Interface (API)
Office of Accountability and Whistleblower Protection	Matter Tracking System (MTS) OAWP Experience API	Performance Code, Performance Review Rating	Application Programming Interface (API)
Office of Performance Analysis and Integrity	Data Management Center PA&I Experience API	Social Security Number, Date of Birth, Sex, Citizenship Code, Veteran Preference, Performance Code,	Application Programming Interface (API)
Enterprise Program Management Office	Occupational Health Record System OHRS Experience API	Resident Address, GSA Code, Social Security Number, Date of Birth, Sex,	Application Programming Interface (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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Race & National Origin Code	
Financial Management Service & iFAMS	Financial Management System / iFAMS (HRPASFMS03)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
Financial Management Service & iFAMS	Financial Management System / iFAMS (HRPASFMS34)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
VISN 1 HR	Electronic Business Operation System (HRPASBOS61)	Social Security Number, Sex, Citizenship Code, Date of Birth, Veterans Preference	Placed in secure AWS S3 bucket.
Retirement Shared Services Office (RSSO)	Government Retirement and Benefits (HRPASGRB27)	Social Security Number, Date of Birth, Resident Address	Placed in secure AWS S3 bucket.
VHA Workforce Management Center (WMC)	VHALWD (HRPASVHA62)	Social Security Number, Sex, Citizenship Code, Performance Rating, Date of Birth, Veteran Preference, Birth Country Code, Type of Visa, Disability Code, Race & National Origin Code	Placed in secure AWS S3 bucket.
Office Business Oversight (OBO)	ProClarity (HRPASOBO73)	Social Security Number	Placed in secure AWS S3 bucket.
Workers Compensation Occupational Safety & Health (WC-OSH)	Workers Compensation Occupational Safety Health Management Information System (HRPASWCP33A)	Social Security Number, Sex, Resident Address, Veterans Preference	Placed in secure AWS S3 bucket.

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Workers' Compensation Occupational Safety & Health (WC-OSH)	Workers Compensation Occupational Safety Health Management Information System (HRPASWCP33B)	Social Security Number, Sex, Resident Address, Veterans Preference	Placed in secure AWS S3 bucket.
Veterans' Health Administration	VistA / Health Informatics (HRPASVIS04)	Social Security Number, Citizenship Code, Performance Code, State Tax, City Tax, Date of Birth, Birth Country, Resident Address	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
Veterans' Health Administration	VistA / Health Informatics (HRPASVIS49)	Social Security Number, State Tax	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)
Financial Management Service	Office of Financial Management Reports (HRPASFMR10)	Social Security Number, Date of Birth, City Tax, State Tax, Resident Address	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)

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:

There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

Mitigation:

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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 shared/received 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***
Veterans Affairs Time and Attendance System (HRPASVAT45)	Financial Services Center	Social Security Number	Two-way transfer using a secure File Transfer Protocol (SFTP) over a Virtual Private Network	ISA-MOU

			(VPN)	
Veterans Affairs Time and Attendance System (HRPASVAT46)	Financial Services Center	Social Security Number	Two-way transfer using a secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ISA-MOU
HR SMART	Human Resources Management Service (HRSHRPAS01)	Name, SSN, date of birth, mailing address, telephone number, email address, emergency contact information, financial account information, taxpayer identification number (TIN), disabilities, criminal record information, service information, Veteran preferences*, student loans, education information, savings plan information and benefit information	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ICD
HRIS	Human Resources Management Service (HRSHRPAS36)	Social Security Number, Race & National Origin, Sex, Disability Code, Citizenship Code, Performance Rating, Date of Birth, Veteran Preference	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ICD
PERSONIFY	American Federation of Government Employees	Social Security Number, Resident Address	Secure File Transfer Protocol (SFTP) over a Virtual Private	National ISA/ MOU

	System (HRPASAFG14)		Network (VPN)	
TALX	Equifax (HRPASTAL32)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	MOU
Personal Identification Verification	Department of Homeland Security HRPASPIV31	Social Security Number, Date of Birth	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	MOU-ISA
Department of Homeland Security	Social Security Administration (SSA) (HRPASSSA40)	Social Security Number, Resident Address, Date of Birth	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ICD
Internal Revenue Service	Social Security Administration (SSA) (HRPASSSA41)	Social Security Number	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ICD
Defense Civilian Pay System (DCPS)	Defense Finance Accounting Service (DFAS) (DCPHRPAS02, DCPHRPAS05, DCPHRPAS06, DCPHRPAS08, DCPHRPAS12, DCPHRPAS13, DCPHRPAS18, DCPHRPAS19, DCPHRPAS20, DCPHRPAS21, DCPHRPAS23, DCPHRPAS26, DCPHRPAS30)	Social Security Number, Resident Address, Disability Retirement Indicator, Performance Code, Performance Review Rating, Disabled Veteran Leave, Birth Country Code, Citizenship Code, Date of Birth, HCP Code, Race & National Origin Code, Sex, Type of Visa, Veteran Preference, VISA Country Code, Primary and Secondary State Tax Marital Status, Federal Income Tax Marital Status,	Two-way connection using Connect Direct Secure+ protocol over a Virtual Private Network (VPN)	MOU-ISA

		City Tax Info, Primary and Secondary State Geographic Code, Primary and Secondary State Residence, Primary and Secondary State Tax, Additional Withholding, Primary and Secondary State Tax Exemptions		
Cerner Clairvia System	Cerner (HRPASCER43)	Resident Address	Secure File Transfer Protocol (SFTP) over a Virtual Private Network (VPN)	ICD
Data Management Warehouse	Enterprise Performance Management System EPMS Full Load Experience API EPMS Delta Experience API	Social Security Number	Application Programming Interface (API)	MOU-ISA
Office of Information & Technology (OI&T) / OCHCO	Safety & Workers Compensation Information Management System (SWIMS) SWIMS Experience API	Social Security Number, Date of Birth, Citizenship Code, Resident Address, Sex, Veteran Preference, Disability Indicator, Disabled Veteran Leave, Marial Status for Federal Income	Application Programming Interface (API)	MOU-ISA

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:
There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation:
The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized for the system.

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.

Respondents/individuals provide human resources data to VA for the purposes of payroll and assessment of employment. This PIA provides additional notice of system's existence and its PII collection, use, maintenance, and dissemination practices. This PIA will available online for public notification, review, and use, as required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii).
System of record Notice (SORN) https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf provides the legal authority and further notice for the collection and use of records pertaining to payroll and human resources. SORN #171VA056A/78 FR 63311(Human Resources Information Systems Shared Service Center (HRIS SSC)-VA)
VA OPRM:

https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.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

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 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

Use of PII described 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:

There is a risk that VA employees will not know that HR-PAS collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation:

The application, through the HR-SMART application (HRIS-SSC) mitigates this risk by ensuring that it provides individuals 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.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the following with below requirements:

- PO or Freedom of Information Act/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.
- The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral. Approved VA authorization forms may be provided to individuals for use.
- Employees or representatives designated in writing seeking information regarding access to VA records may write, email or call the VA office of employment.

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.

HRIS is a self-service system and employees have access to their respective data. Since this is a self- service system, employees can access, redress and correct their own personal and personnel information, and can review and update their respective HR information as necessary. All HRIS users receive an account in PeopleSoft where they can view and update their personal information. Once the account is generated, an email is sent to individuals notifying them of their account.

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.

NOTIFICATION PROCEDURES: Notification for correcting the information will be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. System Manager for the concerned VA system of

records, Privacy Officer, or their designee, will notify the relevant persons or organizations whom had previously received the record about the amendment.

If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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:
Because there is no direct way for individuals to review or correct their information in HR-PAS, there is a risk that the system may use inaccurate data when creating reports.

There is also a risk that individuals whose records contain incorrect information may not receive notification of HR changes. Furthermore, incorrect information in an HR record could result in improper compensation or benefits

Mitigation:
AWS: HR-PAS application resides in a separate account in the Amazon Web Services (AWS) VA government cloud. Direct access to the HR-PAS account from AWS (e.g., to start and stop servers) is controlled via name/password/MFA. A VA administrator assigns roles and controls access to AWS functions.

For individual AWS servers, access is controlled via an e-PAS account and the VA jump servers—this latter access is per individual, and e-PAS accounts must be renewed every 90 days. In addition, AWS provides data encryption for data at rest.

Finally, AWS SFTP services are FIPS 140-2 compliant.

Section 8. Technical Access and Security

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

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

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.

At the project level, security is provided by the Austin Information Technology Center (AITC). Access is granted to individuals with AITC TSO access and written authorization from their supervisor. Facility staff determines level of access for individuals to view and report on their data.

Employees are required to submit VA Form 9957 (Request for Access Form) to the information security office, indicating the requested level of access (Read, Read/Write), and signed by their supervisor. Approval is granted by the facility Information Security Officer and recorded in the Customer User Provisioning System (CUPS).

The HR-PAS staff and several Austin Information Technology Center staff who maintain the HR-PAS system have national access to perform their duties.

VACO staff and Stations have restricted access to HR-PAS data. Stations limited to data for that station.

Access is limited to the scope of responsibility required for each VA employee to perform their duties where it is at VACO or at a station.

HR and Payroll users have access limited to the population of the station they serve.

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 can be granted access to HR-PAS if their VA manager and local Information Security Officer approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form as specified in section 8.1. In addition, in accordance with the contract between the contractor and the government, all contractors with access to HR-PAS information are required to meet the AITC contractor security requirements.

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.

VA provides security and privacy awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by information system changes, and annually thereafter.

In accordance with AITC guidance, AITC personnel that will be accessing information systems 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 VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training.
Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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.

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).*

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.***

Yes, the Security Plan Status is current at Dec 16, 2021 and an Authority To Operate was granted on Feb 26, 2021 for 1 Year expiring Feb 22, 2022.
The Risk Review Completion Date is Sep 10, 2021

The FIPS 199 classification of the system is MODERATE (confidentiality=Moderate, integrity=Moderate, availability=Low).

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.

HR-PAS is hosted in VAEC AWS GovCloud which is a FedRAMP High authorized, and it has a 3-year ATO through agency authorization (VA authorized it).

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.

Infrastructure as a Service (IaaS) model

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.

HRPAS is hosted in VAEC AWS and is covered under the VAEC Enterprise Contract, NNG15SD22B VA118-17-F-2284

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.

No ancillary data is collected

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).

This is the Shared Responsibility Model for Security in the Cloud. HRPAS application owner are responsible for their data.

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

ID	Privacy Controls
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.

Kimberly P. Forte 621462

Digitally signed by Kimberly P. Forte 621462
Date: 2022.01.04 14:40:51 -05'00'

Privacy Officer, Kimberly Forte

Andre L. Davis 1130018

Digitally signed by Andre L. Davis 1130018
Date: 2022.01.04 13:54:12 -06'00'

Information Systems Security Officer, Andre Davis

Dominique A. Banks 747748

Digitally signed by Dominique A. Banks 747748
Date: 2022.01.04 17:03:39 -05'00'

Information Systems Owner, Dominique Banks

APPENDIX A-6.1

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

SORN #171VA056A/78 FR 63311(Human Resources Information Systems Shared Service Center (HRIS SSC)-VA)
VA OPRM:

https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.pdf