Privacy Impact Assessment for the VA IT System called:

Workload and Time Reporting System (WATRS)

Office of Field Operations

Veteran Benefits Administration (VBA)

Date PIA submitted for review:

11/07/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	(202) 632-8423
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000, Ext: 4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Workload & Time Reporting System (WATRS) is a time and production tracking application developed using the Salesforce platform. WATRS allows the VBA employees and supervisors to enter and review time and production entries to support the performance and quality review process. The VA Employee users are on a performance standard that allows them to enter time entries that VA Time and Attendance System (VATAS) does not capture such as deductible time entries thereby reducing any duplicate entries. The time savings of WATRS impacts performance employee's bandwidth giving them more time to work on claims.

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?*

The Workload & Time Reporting System (WATRS) module is built on the Salesforce Government Cloud. The module is managed by the Office of Field Operations (OFO) and AMO and the platform is managed by the Office of Information and Technology (OI&T).

The WATRS module has two components: Time Tracker and Production. Both modules enable the VA employee(s) to log deductible time, premium pay time and production records, which

helps them determine if the falling short of, meeting, or exceeding their own performance standard assigned to them.

The total number of VA employees using the system is over 25,035 with an expectation of growth to 27,000 as additional departments are added in the application. The Production object will contain an unknown number of records where each record will contain a Veteran/ Claimant file number. WATRS application is transitioning to have over 14 user profiles expected to enter Veteran/ Claimant file number of production records. Other user employee types of production records are captured automatically by other case management and production platforms utilized to complete their work (VSRs/RVSRs production records are captured in VBMS and the data is stored outside of Salesforce with the Office of Performance Analysis and Integrity or PA&I)

WATRS system services enterprise wide.

The Time Tracker module does not contain any sensitive or PII information. Time Tracker module is used by all WATRS users to daily adjust their availability by entered deductible time or premium pay time. An example of a deductible time entry is a record that indicates an employee spent one hour in TMS completed a training requirement and was not available for that one hour to work cases. The Production module contains PII information in the form of Veteran/ Claimant file number. The record created by the employee includes the following data: When the Production record was created, who created it, what type of work was completed, and the Veteran/ Claimant file number. The Production record along with the Time Tracker records will paint a picture of the employee's actual performance which they can compare to the performance standard.

Currently only Time Tracker data (non PII data) is transferred daily from Salesforce to a PA&I Secure File Transfer Protocol (SFTP) server. PA&I consolidates the Time Tracker data with other data to create the Employee Performance Report which is visible in the WATRS module. This is a one-way data transfer, and it is facilitated by MuleSoft integration and coding on a DVP server.

To gain access to WATRS users must use of Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

WATRS is covered by the Salesforce Government Cloud Plus Authority to Operate (ATO).

There are no expected changes to the business process or technology based on this PIA.
The SORNs, 'VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28 covers the user of the Veteran/ Claimant file number for production data and 'Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311 covers the time tracking data in the WATRS module

The system does use cloud technology.

Ownership rights to PII data should be covered in the Salesforce contract. Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.

The magnitude of harm if PII was disclosed would have a negative impact on both the Cloud

Service Provider (CSP) and VA. While there is limited data in the system through the Production component, that data could be used to negatively impact individuals' credit, jobs, and other areas sensitive information can be used inappropriately. This could leave the CSP and VA open to litigation.

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)

Site location/ station (can also be referred as Account Name and Address information of duty location), Supervisor Name, District Office, Division/Cost Codes, Tour of Duty (VBA allows flex and compressed schedules i.e. 5 days/8hrs; 4 days/10hrs, etc.,), QMS Information (QMS User, Review Level, Available Review Types) – On hold for clarification, Grade Scale (GS) Grade (GS Level), EIN (Unique Employee ID in lieu SSN), LAN ID (log-in ID should SSO), User ID (WIT ID or unique VBA ID), Role (Level of access per employee i.e. National or local), Federation ID/work email address, Position/Title, Experience Level in months, Number of Days per Pay Period of Telework, Production Performance Standards, Availability (Excluded Time), Veteran/Claimant file number.

PII Mapping of Components

Workload & Time Reporting System (WATRS) consists of 1 key components (databases). If WATRS did contain components, then each component would have been analyzed to determine if any elements of that component collect PII. The type of PII collected by Workload & Time Reporting System (WATRS**)** and the reasons for the collection of the PII are in the table 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
Enterprise Data Warehouse (EDW)	Yes	Yes	Veteran/ Claimant File Number, Veteran SSN Employee information: Name, Site location, User ID, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title, Experience Level in Months, Federation ID/work email address	Enterprise Data Warehouse (EDW) server used to validate the VA employees information during their tenure within the VA and also validate the employee performance standards	Internal connection between two servers via bi-directional connectivity. Site-to-site encrypted transmission

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.

The information in WATRS is collected directly from the VA employees. Two types of information are entered into the WATRS portal, production hours and excluded time reporting hours. For production hours or record type, an employee must enter the Veteran/ Claimant file number that corresponds to the Veteran/Claimant whose case they worked on to receive credit. For time tracking, employees input the time spent in hours to track active work-time hours, additional time hours spent on administrative tasks and excluded time availability. WATRS does not interact with data sources external to the VA user.

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.

The information is collected directly from the VA employees. An employee creates a production record in WATRS by entering the Veteran/ Claimant file number pertaining to the Veteran record to receive credit and /or time record by entering the excluded time hours available.

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 correct entry of a Veteran/ Claimant file number is completely dependent on the end user entering it correctly. A random sample of the production records for quality review purposes will ensure that those records reflect a correct Veteran/ Claimant file number. This will be done at frequency set by quality reviewers for production records being created in WATRS. If an incorrect Veteran/ Claimant file number is entered, incorrect associated data will not be retrieved. This is because the module at this time does not pull associated data/records with the entry of a Veteran/ Claimant file number.
Time record entered by individual employee is confirmed by the supervisor on the WATRS portal. Time hours is checked bi-weekly by the supervisor.

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 WATRS module is covered under the overarching Salesforce Government Cloud Plus authority to operate. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

As per the SORN,

1. Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311, the authority of maintenance of the system listed in question 1.1 falls under 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.
2. VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28, the authority of maintenance of the system listed in question 1.1 falls under Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

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: The risk is similar with any other systems that if the wrong person were to have access to the information, it could be used to obtain financial resources and negatively impact a beneficiaries' lives.

Mitigation: The Salesforce Government Cloud requires all access utilize a PIV card while also logged onto the VA network through secure sites essentially a 2-factor authentication process. All VA employees accessing the system have had full background checks. Additionally, no external users will have access to this Salesforce module. Finally, the Veteran/ Claimant file number field will be encrypted per FIPS 140-2 Security Requirements.

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.

Information of Veteran/VA Employees collected by WATRS tool are:

- Veteran/ Claimant File Number: an employee must enter the Veteran/ Claimant file number that corresponds to the Veteran/Claimant whose case they worked on to receive credit.
- Veteran SSN: Validate the information of the Veteran associated with the Veteran/ Claimant file number.
- Name: used to identify the employee
- Site location/ station: also referred to as account name and address/location information of duty location.
- Grade Scale (GS) Grade (GS Level): used to identify the scale of quality reviews provided to individual VA employees.
- User ID (WIT ID or unique VBA ID): unique ID provided to individual employee, used to track the time and production hours of the employee in the system
- Role: level of access grated to use the WATRS portal per employee. National or local, admin access to user access.
- Federation ID/ work email address: to identify the employee.
- EIN (Unique Employee ID in lieu SSN): unique ID used instead of SSN
- LAN ID (log-in ID should SSO): used as an alternate for login-in
- Position/ Title: used to track the responsibilities and to evaluate performance standards
- Production Performance Standard: used for evaluation of production hours.
- Experience Level in months: used to identify the qualification and for evaluation of performance standards
- Production and Availability (Time): used to monitor the production hours and time availability of the employee for scheduling
- Number of Days per Pay Period of Telework: used to identify the type of work assigned to employee.
- Availability (excluded time): used for tracking the available time hours spent on administrative tasks
- Supervisor Name: also the employee reporting personnel. used to validate the time hours of VA employee.
- District Office: district to which individuals are signed under
- Division/Cost Codes: assigned to track the codes to which individual employee is billed
- Tour of Duty (VBA allows flex and compressed schedules i.e. 5 days/8hrs; 4 days/10hrs, etc.,): to track the compressed schedule hours of individuals
- QMS Information (QMS User, Review Level, Available Review Types): used for validation and quality of veteran/claimant work credit to be assigned for individual employee.

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 Production component does not do analytics on individuals. A dashboard will be utilized to summarize the Production records for the employee but will not include Veteran/ Claimant file number information.

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

WATRS (Salesforce) is an encrypted secure system. Data in transit are protected by HTTPS site-to-site encryption. PII data are encrypted at rest with Salesforce Shield encryption. SSN is PII data, encrypted at rest with Salesforce Shield encryption.

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.

New users submit a request for access through the Digital Transformation Center (DTC). The DTC then assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce.

Any disciplinary actions for misuse of the information would be covered in VBA's privacy policy and by governing regulations.

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

Veterans/ VA employee's information retained by WATRS tool are:
Veteran/ Claimant File Number, Veteran SSN, Name, site location/ station (can also be referred as account name and address information of duty location), supervisor name, district office, division/cost codes, tour of duty (VBA allows flex and compressed schedules i.e. 5 days/8hrs; 4 days/10hrs, etc.,), QMS information (QMS user, review level, available review types) – on hold for clarification, grade scale (GS) grade (GS level), EIN (unique employee ID in lieu SSN), LAN ID (log-in ID should SSO), User ID (WIT ID or unique VBA ID), role (level of access per employee i.e. national or local), Federation ID/work email address, position/title, experience level in months, number of days per pay period of telework, production performance standards, availability (excluded time)

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.

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record

Control Schedule 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

Information Technology Operations and Maintenance Records. Disposition instructions: Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

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 below is the retention schedule for the Salesforce Government Cloud Plus (SFGCP) and applies to the WATRS module as well. SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

SFGCP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older than 90 days is unrecoverable. VA can export the data stored on the SFDP and retain it locally in order to meet VA/NARA retention requirements.

Information Technology Operations and Maintenance Records. Disposition Authority: AA-GRS-2013-0005- 0004, item 020. Disposition instructions: Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

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

All records will be electronic, and the details of their disposal will be documented within the SORN and should also be recorded as part of the Software as a Service (SaaS) documentation/contract. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500 (https://www.va.gov/vapubs/search_action.cfm?dType=1).

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. 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 lower development environments for Salesforce do not allow the use of PII. For the Production component, test data is utilized/created. Because the configuration of the component does not have any validation against other VA systems of record, real Veteran data is not required to test the functionality of the system. Training for users is done in the lower environments and test data is used.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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: The risk to maintaining data within WATRS is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached

Mitigation: To mitigate the risk posed by information retention, the WATRS Module adheres to the VA RCS schedules for each category or data it maintains. The WATRS module would follow the overall strategy of SFGCP as outlined in the PIA. When the retention data is reached for a record, the Care Now team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA Care Now records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Performance Analysis and Integrity (PA&I)	Used for validating the employee performance standards	Employee Time Tracking, Production Information, Quality Management System Information	WATRS sends to PA&I through secured FTP sites
Office of Information Technology / Enterprise Program Management Office (EMPO): EPMD Enterprise Services	MuleSoft, formerly Digital Veterans Platform (DVP). Used as a connection between PA&I and WATRS.	Veteran/ Claimant File Number, Veteran SSN Employee: Name, Site location, User ID, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title, Experience Level in Months, Federation ID/work email address	Internal connection between two servers via bi-directional connectivity. SFTP implemented transfer data back and forth from Salesforce to another VA system using DVP.
Office of Information Technology / Enterprise Program Management Office (EMPO): EPMD Enterprise Services	Secure File Transfer Protocol (SFTP) server. Used as a connection between PA&I and WATRS.	Veteran/ Claimant File Number, Veteran SSN Employee: Name, Site location, User ID, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title, Experience Level in Months, Federation ID/work email address	Internal connection between two servers via bi-directional connectivity. SFTP implemented transfer data back and forth from Salesforce to another VA system using DVP.
Office of Information Technology / Enterprise Program Management Office (EMPO): EPMD Enterprise Services - Enterprise Data Warehouse (EDW) server	Enterprise Data Warehouse (EDW) server used to validate the VA employees information during their tenure within the VA and also validate the employee performance standards	Veteran/ Claimant File Number, Veteran SSN Employee: Name, Site location, User ID, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title, Experience Level in Months, Federation ID/work email address	Internal connection between two servers via bi-directional connectivity. SFTP implemented transfer data back and forth from Salesforce to another VA system using DVP.

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*

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: The risk is similar with any other systems that if the wrong person were to have access to the information, it could be used to obtain financial resources and negatively impact a beneficiaries' lives.

Mitigation: The Salesforce Government Cloud requires all accessors utilize a PIV card while also logged onto the VA network through secure sites essentially a 2-factor authentication process. All VA employees accessing the system have had full background checks. Information is only shared with approved internal systems. Security controls are in place to prevent unauthorized access such as: access controls, authentication, and use of PIV. Audit logs in Salesforce are available to track any inappropriate internal sharing and/or disclosure.

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	N/A	N/A	N/A	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: N/A

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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.

Yes, VA employees are aware of the time and production hours being tracked by the WATRS tool. The Department of Veterans Affairs provides notice that the system exists. This is done in two (2) ways:

1. Through the SORNS Published in the Federal Register:
    a. 171VA056A/78 FR 63311 - Human Resource Information Shared Service Center (HRIS SSC) – VA.
    b. 58VA21/22/28 86 FR 61858 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.
2. This Privacy Impact Assessment (PIA) also serves as notice of the system. As required by the eGovernment Act of 2002, Pub.L.107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment

publicly available through the website of the agency, publication in the Federal Register, or other means."

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

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

VA Employees do have the option of declining the information. Updating WATRS is a condition of the VA employees 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

Users consent to the uses of the data within the tool via the login portal. A snapshot of the relevant text is noted below:

All transactions, including searches and record views, that occur on this system, and all data transmitted through this system, are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: The risk is associated with employees being unaware the data is being captured by the WATRS tool.

Mitigation: The users accessing the WATRS tool consent to the data usage as described in 6.3.

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 data collected within the Production component is not exempt from FOIA/Privacy Act requests and would be handled by the centralized group processing VBA FOIA/Privacy Act requests.

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.

If a wrong Veteran/ Claimant file number is entered by an employee on the Production record, that employee would have the ability to edit the Veteran/ Claimant file number field to make any corrections as necessary.

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.

The employees can correct their own records if needed. If the record is selected for a quality review, then the quality reviewer can potentially notify the employee to correct the Veteran/ Claimant file number. The employee's supervisor would be able to notify the employee as well if a Veteran/ Claimant file number needs to be corrected.

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.

This is not applicable to WATRS.

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: No specific risks are identified as the information collected in the Production component is only utilized to identify the Veteran/Claimant. The information collected is not used to grant, adjust, or deny benefits and incorrect information contained in the system has no negative impact on the beneficiary.

Mitigation: If PII is listed incorrectly in the WATRS module, the end user would be able to correct the record accordingly ensuring the only accurate information persists in the WATRS module.

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.

Beneficiaries do not have direct access into the Case/Feedback component within the Salesforce platform.

New users submit a request for access through the Digital Transformation Center (DTC). The DTC then assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the admin's response.

No users from agencies outside VBA have access to WATRS within the Salesforce platform in the production environment. The VBA employees are able to edit entries that were part of the original submission as well as other items needed for case management and workload reporting.

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.

Only VA contractors from the DTC will have access to the production environment. Details surrounding their credentialing and training for access as the support contractors for the Salesforce platform will have to be provided by OIT.

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

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

General Training includes VA Privacy Rules of Behavior, Privacy awareness training, and VA on-boarding Cyber Security enterprise-wide training within Talent Management System (TMS). No additional system specific privacy training is provided for end users of WATRS.

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.***

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 02/24/2021
3. The Authorization Status: ATO

4. The Authorization Date: 03/18/2021
5. The Authorization Termination Date: 12/17/2023
6. The Risk Review Completion Date: 03/12/2021
7. The FIPS 199 classification of the system – Moderate

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.

Yes, WATRS utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This is under the contract: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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.

Yes, VA has full ownership of the PII that will be used by WATRS platform. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

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.

No ancillary data is being collected by WATRS.

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.

Yes, as VA is utilizing Salesforce Gov Cloud Plus. Information is only shared internally.

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).

WATRS salesforce module does not utilize RPA.

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 they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.12.05 15:02:45 -05'00'

Privacy Officer, Tonya Facemire

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.12.07 10:26:32 -05'00'

Information System Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.12.07 10:17:24 -05'00'

Information System Owner, Michael Domanski

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).

OPRM website for SORN: https://www.oprm.va.gov/privacy/systems_of_records.aspx

VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA, 58VA21/22/28 (2021-24372.pdf (govinfo.gov))

Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311 (2013-24830.pdf (govinfo.gov))

Record Schedule 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

NARA website link

VA Directive 6500: VA Publication