Privacy Impact Assessment for the VA IT System called:

Salesforce – Workload and Time Reporting System

Veterans Benefits Administration

Office of Field Operations

eMASS ID # 2037

Date PIA submitted for review:

06/20/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	Lakisha.Wright@va.gov	(202) 632-7216
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?".

The Workload & Time Reporting System (WATRS) is a time and production tracking application developed using the Salesforce platform. WATRS/WATRS -Production allow 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 GovTA (formally, the 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:

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

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 by the Office of Information and Technology (OI&T).

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

The Workload & Time Reporting System (WATRS) is a time and production tracking application developed using the Salesforce platform. WATRS is currently being used by over 25,011 Veterans Benefits Administration (VBA) employees and supervisors with an expectation to grow to 27,000 as additional departments are added to the application. 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 requires them to enter time entries that GovTA does not capture, such as deductible time entries thereby reducing any duplicate entries. The time savings would impact performance employee's bandwidth giving them more time to work on claims.

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 they are falling short of, meeting, or exceeding their own performance standard.

C. *Who is the owner or control of the IT system or project?*

Salesforce Government Cloud Plus (SFGCP) is a cloud platform, data in the platform is controlled by VA but non-VA Owned and Operated. 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.

2. Information Collection and Sharing

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

The total number of VA employees using the system is over 25,011 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 has 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. These production records are captured, and the data is stored, outside of Salesforce with the Office of Performance Analysis and Integrity (PA&I).

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

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 requires them to enter time entries that GovTA does not capture such as deductible time entries thereby reducing any duplicate entries. The time savings would impact performance employee's bandwidth giving them more time to work on claims.

The WATRS module has two components: Time Tracker and Production.

- 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 completing 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 help the employee’s actual performance which they can compare to the performance standard. Both modules enable the VA employee(s) to log deductible time, premium pay time, and production records, which helps them determine if they are falling short of, meeting, or exceeding their own performance standard.

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

Currently, WATRS pushes data to the Performance Analysis & Integrity tool (PA&I) which will allow for future enhancements of the data to be sent and made available to the Quality Management System (QMS). Additional enhancement to WATRS will allow for increased efficiency in adding new user groups that are transitioning to WATRS thereby reducing onboarding time for new users.

Workforce Information Tool (WIT) integration through MuleSoft as a middleware will enable auto-provisioning of information being pulled into WATRS module on a daily basis.

In addition, integration with the Corporate Data Warehouse (CDW) will be made to retrieve GovTA premium time, union time, leave time, and schedules to duplicate into WATRS.

G. *Is 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?*

Yes, WATRS system services is enterprise wide. File Number is the only PII information which will be consistent throughout WATRS application. Veteran/ Claimant File Number is validated through CDW/PA&I systems to ensure consistency. To gain access to WATRS application, users must use of Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

Two SORNs provide the legal authority to operate the IT system,

1. 'VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28 2021-24372.pdf (govinfo.gov) covers the user of the Veteran/ Claimant file number for Production data 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.
2. 'Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311 covers the time tracking data in the WATRS module 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.

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

No, the SORN does not require amendment. The WATRS system does utilize cloud technology, the SORN listed below covers the cloud usage or storage.

1. 'VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28 (2021-24372.pdf (govinfo.gov))
2. 'Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311

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.

4. System Changes

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

The completion of this PIA will not result in changes to business process.

K. *Will the completion of this PIA could potentially result in technology changes?*
WATRS is a web-based application. New integrations which include MuleSoft as a middleware, accessing the CDW to use tables with GovTA (formerly known as VATAS) data to automatically create matching downtime entries in WATRS, and accessing data from the WIT object to update user contact records which will result in technological changes.

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

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

☒ Name
☒ Social Security Number
☐ Date of Birth
☐ Mother’s Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

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

Other PII/PHI data elements:
- 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.,)
- Quality Management System Information (QMS User, Review Level, Available Review Types)
- 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 in lieu of SSN)
- Role (Level of access per employee i.e. National or local)
- Federation ID/Work email address
- Position/Title
- Experience Level in months
- Employee time tracking such as - Number of Days per Pay Period of Telework, production Performance Standards, Availability (Excluded Time), Premium time requests, Union time data, Leave Data
- For the WATRS – Production module only we also use:
    - Date of production action, action type, number of production items
    - Claim related information (date of claim, claim label, file number (SSN or unique identifier), number of issues, claim processing priority level, end product, and mail packet number)
    - Benefit claim ID (unique identifier of claim separate from Veterans SSN).

PII Mapping of Components (Servers/Database)

Salesforce – Workload & Time Reporting System (WATRS) consists of four key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by WATRS and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Enterprise Data Warehouse (EDW/VD2)	Yes	Yes	Veteran/ Claimant File Number, Veteran SSN. Employee: Name, Site location, User ID, LAN ID,	Enterprise Data Warehouse (EDW) server used to validate the	Internal connection between two servers via bi-directional connectivity. SFTP implemented transfer data back and forth from

			Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title, Experience Level in Months, Federation ID/work email address	VA employee’s information during their tenure within the VA and also validate the employee performance standards	Salesforce to another VA system using DVP.
Workforce Information Tool (WIT)	Yes	Yes	Employee Name, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Role, Position/Title, Experience Level in Months, Federation ID/work email address, email address	The Workforce Information Tool (WIT) provides all necessary data for provisioning of users. Data within the WIT is used to provide the data keys when mapping performance and time data between systems.	WIT permissions are limited to information in the WIT object. Data from WIT is pulled to update user records in WATRS application.
Corporate Data Warehouse (CDW)	Yes	Yes	Employee 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, Leave Data, email address, Tour of duty, Premium	Office of Accountability and Whistleblower Protection (OAWP) Finding Data is collected to create duplicate entries into WATRS automatically, so users do not have to manually enter them.	SFTP or HTTPS

			time requests, Union time data.		
Salesforce Government Cloud Plus (va.my.salesforce.com) platform	Yes	Yes	Veteran information: Veteran/ Claimant File Number, Veteran SSN, Benefit Claim ID, Claim related information: Date of Claim, claim processing priority level, claim label, number of issues/claims, mail packet number VA Employee/Contractor related information: 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.,), Quality Management System Information (QMS User, Review Level, Available Review Types), Grade Scale (GS) Grade (GS Level), EIN (Unique Employee ID in lieu SSN), Employee SSN, LAN ID (log-in ID should SSO), User ID (WIT ID or unique VBA ID in lieu of SSN), Role (Level of access per	Underlying platform that allows VBA employees and supervisors to enter and review time and production entries to support the performance and quality review process,	Minor system contained in a cloud container of SFGCP platform but do not share data with the container

			employee i.e. National or local), Federation ID/Work email address, Position/Title, Experience Level in months, Email address, Employee time tracking (such as, Number of Days per Pay Period of Telework, production Performance Standards, Availability (Excluded Time), Premium time requests, Union time data, Leave Data), Other WATRS Production data (such as, date of production action, action type, number of production items, number of issues, claim processing priority level).		

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

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

The production information in WATRS is collected directly from the VA employees. Two types of information are entered into the WATRS module production entries and time reporting hours. For production entries, 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, except as identified below.

Workforce Information Tool (WIT) integration through MuleSoft as a middleware will enable auto-provisioning of information being pulled into WATRS module on a weekly to daily basis. Integration with the Corporate Data Warehouse (CDW) will be made to retrieve GovTA premium time, union time, leave time, and schedules to duplicate into WATRS which enables validation of VA employee's information during their tenure within the VA and their performance standards.

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

This is not applicable since information is collected directly from the VA employees.

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

WATRS application tracks the production hours and excluded time hours. The Production WATRS module creates the performance reports based on information entered by employees and used for their performance standards.

1.3 How is the information collected?

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

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

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. Additionally, their time is tracked by time records by entering the excluded time hours available.

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

Information is not collected on paper; hence this is not applicable to WATRS.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The 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 at a minimum bi-weekly by the supervisor.

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

WATRS does not utilize commercial aggregators since the information is provided directly by the end user, VA Employees, to report their time hours spent claims processing.

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

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

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 (2021-24372.pdf (govinfo.gov), 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 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

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

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

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

<u>Privacy Risk</u>: 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 Veteran or beneficiary.

<u>Mitigation</u>: 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/contractors 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
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.	Not used
Veteran SSN	Validate the information of the Veteran associated with the Veteran/ Claimant file number.	Not used
Benefit Claim ID	unique identifier of claim separate from Veteran SSN	Not used

Claim related information: date of claim, claim processing priority level, claim label, number of issues/claims, mail packet number	Identify the Veteran/claimant related issues.	Not used
Name	Used to identify the employee/ contractor	Not used
Site location/ station	also referred to as account name and address/location information of duty location.	Not used
Supervisor Name	VA employee reporting personnel. used to validate the time hours of VA employee/ contractor.	Not used
District Office	District to which individuals are signed under	Not used
Division/Cost Codes	Assigned to track the codes to which individual employee is billed	Not used
Tour of Duty (VBA allows flex and compressed schedules i.e. 5 days/8hrs; 4 days/10hrs, etc.,)	To track the schedule hours of individuals	Not used
QMS Information (QMS User, Review Level, Available Review Types)	Used to determine QMS workload and reporting.	Not used
Grade Scale (GS) Grade (GS Level)	Used to identify the production plan associated to individual VA employees	Not used
EIN (Unique Employee ID in lieu SSN)	Unique ID used instead of SSN	Not used
Employee SSN	Used to identify VA Employee/contractors when EIN is not available	Not used
LAN ID (log-in ID should SSO)	Used as an alternate for login-in	Not used
User ID (WIT ID or unique VBA ID)	Unique ID provided to individual employee, used to track the time and production hours of the	Not used

	employee/ contractor in the system	
Role	Level of access grated to use the WATRS portal per employee/ contractor. National or local, admin access to user access.	Not used
Federation ID/ work email address	To identify the employee/ contractor.	Not used
Position/ Title	Used to track the responsibilities and to evaluate performance standards	Not used
Experience Level in months	Used to identify the qualification and for evaluation of performance standards	Not used
Production Performance Standard	Used for evaluation of production hours.	Not used
Production and Availability (Time)	Used to monitor the production hours and time availability of the employee for scheduling	Not used
Number of Days per Pay Period of Telework	Used to identify the type of work assigned to employee.	Not used
Availability (excluded time)	Used for tracking the available time hours spent on administrative tasks	Not used
Other WATRS Production data such as, date of production action, action type, number of production items.	Used to monitor the production hours of employees and track associated tasks	Not used

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

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

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

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

Performance records are created for employees in WATRS -Production and data is used from WATRS in the EPR program that would be used to grade employees performance in their duties and this is accessible by management who have access to the WATRS application.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

WATRS is accessed via a secured webpage utilizing Single Sign On (SSO) technology. WATRS application is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. The data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Product provides FIPS 140-2 certified encryption.

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

Fields such as SSN are protected by Salesforce Shield Protect which provides FIPS 140-2 certified encryption. The two SORNs (Human Resource Information Shared Service Center (HRIS SSC) – VA, 171VA056A/78 FR 63311, and VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28 (2021-24372.pdf (govinfo.gov)) defines the information collected for Veterans, use of the information, and how the information is access and stored. WATRS application captures VA employees time hours spent assisting the Veteran and the remaining time hours.

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

WATRS is accessed via a secured webpage utilizing SSO technology. WATRS tool is implemented with the 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.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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

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

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

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

2.4a How is access to the PII determined?

Users are provided access to PII only on a need-to-know basis to execute/ facilitate a work tracking request within the WATRS application or record hours. Profile based settings is applicable to the tool limiting the type of information accessed by individual users authenticated by PIV Single Sign On (SSO). Additionally, the SORN defines the use of the information and how the information is accessed, contained, and stored in the system.

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

New users submit a request for access through the Digital Transformation Center (DTC). 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 by the admin. DTC is then notified of the approval/disapproval and DTC acts on the request based on the admin’s response. Requests, approvals, and denials of access are recorded within Salesforce.

2.4c Does access require manager approval?

Yes, supervisor/ managerial approval, referred to as admin access in 2.4b, is required for new users accessing WATRS application.

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

Profile based settings is applicable to the tool limiting the type of information accessed by individual users authenticated by PIV Single Sign On (SSO). User have limited access to PII information captured in the tool and access is monitored using logging details available through Salesforce cloud technology.

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

WATRS is accessed via a secured webpage utilizing SSO technology. WATRS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is applied based on FedRAMP Salesforce Gov Cloud Plus (SFGCP) platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.

WATRS Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards are put in place to protect PII and other sensitive information. 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*

Following information is retained in WATRS application:

- Veteran/ Claimant File Number (may be SSN for older Veteran)
- Benefit Claim ID
- Claim related information (date of claim, claim processing priority, level, claim label, number of issues/claims, mail packet number)
- VA employee/ Contractor Name
- VA employee/ contractor site location/ station (can also be referred as account name and address information of duty location)
- VA employee/ contractor supervisor name
- VA employee/ contractor district office
- VA employee/ contractor division/cost codes
- VA employee/ contractor tour of duty (VBA allows flex and compressed schedules i.e. 5 days/8hrs; 4 days/10hrs, etc.,)
- VA employee/ contractor QMS information (QMS user, review level, available review types),
- VA employee/ contractor grade scale (GS) grade (GS level)
- VA employee/ contractor EIN (unique employee ID in lieu SSN)
- VA employee/contractor SSN
- VA employee/ contractor LAN ID (log-in ID should SSO)
- VA employee/ contractor User ID (WIT ID or unique VBA ID)
- VA employee/ contractor role (level of access per employee i.e. national or local)
- VA employee/ contractor Federation ID/work email address
- VA employee/ contractor position/ title
- VA employee/ contractor experience level in months
- VA employee/ contractor time tracking such as – number of days per pay period of telework, production performance standards, availability (excluded time), premium time requests, union time data, leave data.
- Other WATRS Production data such as, date of production action, action type, number of production items.

3.2 How long is information retained?

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

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

Item# 2000.2, Title: 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.

The SORN, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA. 58VA21/22/28 (2021-24372.pdf (govinfo.gov)) provides the retention time for the system as follows, Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA. VB-1 document is located at Guides and Pamphlets - Web Automated Reference Material System (va.gov)

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

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

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

WATRS complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the WATRS instance will be retained as long as the information is needed in accordance with VA Records Control Schedule VB–1, Part 1. Specific retention periods can be located in the VB-1 document at the following URL: https://www.benefits.va.gov/WARMS/21guides.asp

The retention schedule for the Salesforce Government Cloud Plus (SFGCP) also applies to the WATRS module as well.

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

Records will be maintained and disposed of in accordance with VA Directive 6300. VA will use NARA regulations mentioned in VB-Part 1 of managing electronic records as follows,

1. Item# 2000.2, Title: 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.

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 SFGCP and retain it locally in order to meet VA/NARA retention requirements.

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

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

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. 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.

<u>3.6 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

<u>Privacy Risk</u>: The risk to maintaining data within WATRS as the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

<u>Mitigation</u>: 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 such as - Number of Days per Pay Period of Telework, production Performance Standards, Availability (Excluded Time), Premium time requests, Union time data, Leave Data Other WATRS Production data such as (date of production action, action type, number of production items) Quality Management System (QMS) Information (QMS User, Review Level, Available Review Types)	WATRS sends to PA&I through secured FTP sites
Office of Performance Analysis and Integrity (PA&I) WIT	Used to update employees contact records	Employee: Name, Site location, User ID, LAN ID, Supervisor Name, District Office, Division/Cost Codes, GS Level, Tour of Duty, Role, Position/Title,	Data pulled from the WIT object through internal

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***
		Experience Level in Months, Federation ID/work email address	connection SFTP.
Office of Information Technology / Enterprise Program Management Office (EMPO): EPMD Enterprise Services - MuleSoft, formerly Digital Veterans Platform (DVP)	MuleSoft, formerly Digital Veterans Platform (DVP). Used as a connection between PA&I and WATRS.	Only metadata is captured in the MuleSoft Gov Cloud API.	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	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	Enterprise Data Warehouse (EDW) server used to validate the VA employees information during their tenure within the VA and also validate the	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,	Internal connection between two servers via bi-directional connectivity.

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***
Warehouse (EDW/VD2) server	employee performance standards	Role, Position/Title, Experience Level in Months, Federation ID/work email address	SFTP implemented transfer data back and forth from Salesforce to another VA system using DVP.
Corporate Data Warehouse (CDW)	Used to validate the VA employees information during their tenure within the VA and also validate the employee performance standards	Veteran/ Claimant File Number, Employee 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, Leave Data, email address, Tour of duty, Premium time requests, Union time data	SFTP or HTTPS
Salesforce – Quality Management System	For validating the action completion of VA employees/contractor.	VA Employee/contractor information - Quality Management System Information (QMS User, Review Level, Available Review Types)	Site-to-site encrypted transmission

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The 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 Veterans life.

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?
1)
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 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

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

Follow the format below:

<u>Privacy Risk</u>: The risk pertains to unauthorized users accessing the information which could negatively impact the Veterans.

<u>Mitigation</u>: No data is shared externally.

Section 6. Notice

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

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

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

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

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."

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

Notice is provided as described in 6.1a.

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

Notice is provided as described in 6.1a.

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 to provide 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<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:

<u>Privacy Risk</u>: The risk is associated with employees being unaware the data is being captured by the WATRS tool.

<u>Mitigation</u>: 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?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be***

listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

Per the SORN, ‘‘Human Resources Information System Shared Service Center (HRIS SSC)—VA’’ (171VA056A), Employees or representatives designated in writing seeking information regarding access to VA records may write, email or call the VA office of employment.

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

WATRS application is not exempt from Privacy Act.

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

Veterans, VA employees and VA contractors can gain access to their information through FOIA described in section 7.1a.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

This is not applicable to WATRS as employees are using the system to capture their time reporting. Individuals can gain access to their information as explained in 7.1a.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk</u>: No specific risks are identified as the information collected is of VA employees and contractor's workload and time reporting, who are the users of the application.
In WATRS Production, fields associated to identify the Veteran/Claimant is captured. The Veteran/ Claimant may not be aware their information is captured in the application.

<u>Mitigation</u>: If PII is listed incorrectly in the WATRS module, the end user (VA employee or contactor) would be able to correct the record accordingly ensuring only accurate information persists in the WATRS module.
The information collected on Veteran/Claimant is not used to grant, adjust, or deny benefits and incorrect information contained in the system has no negative impact on the beneficiary. They can request access to their information as described in section 7.1a

Section 8. Technical Access and Security

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

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

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

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

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). DTC then assigns the request to the managers having admin access to the module who then determine approval/denial based on the information provided by the user. DTC then acts on these requests based on the admin's response and notifies the new user on the approval/disapprovals.

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

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.

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

Following are the roles and access for WATRS application.

Role	Responsibilities and Access Type
Employee	Enter Time with last 4 days for self
Supervisor	Review/Enter Time and approve or deny within last 14 days.
Division level	Access to all records across divisions at the Regional Office. This role sits higher than all at the station. Bypass Validations Checkbox (Contact Record) – This allows user to modify time entries past 14 days.

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.

VA contract employee from the DTC and possibly from the contract being managed by the Contracting Officer's Representative (COR). Access is verified through the (COR) and other VA supervisory/ administrative personnel before contractors are granted to any VA system.

Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/ Program Manager, and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

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

General Training includes: VA Privacy Rules of Behavior, Privacy awareness training, HIPPA and VA on-boarding enterprise-wide training. 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 part of the 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. System administrators are required to complete additional role-based training. All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06-21-2022
3. *The Authorization Status:* Active

4. *The Authorization Date:* 06-26-2023
5. *The Authorization Termination Date:* 06/26/2026
6. *The Risk Review Completion Date:* 07/06/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

This is not applicable.

Section 9 – Technology Usage

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

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

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

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

Yes, WATRS utilizes Salesforce Gov Cloud Plus - Enterprise. 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. MuleSoft middleware integration allows dataflow through different systems.

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

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 application.

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).

Salesforce - WATRS 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**
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.

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.07.24 07:18:37 -04'00'

Privacy Officer, Lakisha Wright

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.07.31 08:13:44 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.08.01 11:08:11 -04'00'

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; screen shot of a website collection privacy notice).

SORNs applicable for the system:

1. 'VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA' 58VA21/22/28 2021-24372.pdf (govinfo.gov)
2. 'Human Resource Information Shared Service Center (HRIS SSC) – VA' 171VA056A/78 FR 63311

Records Control Schedule, VB-1 - Guides and Pamphlets - Web Automated Reference Material System (va.gov)

HELPFUL LINKS:

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices