Privacy Impact Assessment for the VA IT System called:

Salesforce: NCA Workload & Time Reporting System (NCA WATRS)

National Cemetery Administration

Field Programs, Memorial Products Services-Headstone and Marker units

eMASS ID: 2039

Date PIA submitted for review:

01/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Cindy Merritt	cindy.merritt@va.gov	321-200-7477
Information System Security Officer (ISSO)	James Boring	james.boring@va.gov	215-842- 2000, Ext: 4613
Information System Owner	Mike Domanski	michael.domanski@va.gov	727-595-7291

Abstract

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

This Salesforce solution will be an iteration of the existing Workload and Time Reporting System (WATRS) currently being used by VBA. The NCA WATRS tool will track production records with employee time availability within the National Cemetery Administration. Supervisors will be able to actively track employee production against their assigned hours to determine any opportunities or gaps that would allow for additional support to ensure that commitments are made in a timely manner. The NCA WATRS tool will be reducing the time and effort of the supervisor to gather productivity hours of individual employee thereby facilitating a quicker reporting and feedback to the leadership and/ or employees' assignment or hiring.

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?*

Salesforce: NCA Workload & Time Reporting System (NCA WATRS) is controlled by the Field Programs, Memorial Products Services- Headstone and Marker units within the National Cemetery Administration.

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

This Salesforce solution will be an iteration of the existing Workload and Time Reporting System (WATRS) currently being used by VBA. The NCA WATRS tool will track production records with employee time availability. Supervisors will be able to actively track employee production against their assigned hours to determine any opportunities or gaps that would allow for additional support to ensure that commitments are made in a timely manner. The NCA WATRS tool will be reducing the time and effort of the supervisor to gather productivity hours of individual employee thereby facilitating a quicker reporting and feedback to the leadership and/ or employees' assignment or hiring.

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

Salesforce is a cloud platform. Data in Salesforce Government Cloud Plus (SFGCP) is Veterans Affairs Controlled and non-VA Owned and Operated.

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?*

Approximately 40 employees and the information stored will be their performance data and time accounting.

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

Salesforce: NCA Workload & Time Reporting System (NCA WATRS) track employee production and time availability against performance standards for individual employees initially within its Memorial Product Service, Headstone and Marker Unit, First Notice of Death unit, NCA Appeals, and Presidential Memorial Certificate. The tool collects data of the employee's first and last name, assigned site, unique Employee User ID created by the team for internal tracking, General Schedule (GS) pay scale, and assigned employee tour of duty (scheduling full time or part time status), veteran ID – an auto generated non-PII field captured by AMAS. The tool is said to be used by 40 VA employee users .

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

The tool has two internal connections: Automated Monument Application System (AMAS) and VA Time and Attendance System (VATAS). AMAS data includes the information about memorial products ordered, replacement rate, and processing timeliness. VATAS is leave and premium time records for employees.

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?*

Multiple locations - all employees are now remote. PII is maintained consistently at all sites and with same controls.

3. Legal Authority and SORN

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

The NCA 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. https://www.federalregister.gov/documents/2023/06/28/2023-13681/privacy-act-of-1974-system-of-records

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. Additional authority is 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.

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. Yes, the SORN listed covers the cloud usage or storage; 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.

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?
No, the completion of this PIA will not result in technology 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: Assigned site location/site name, General Schedule (GS) pay scale, Unique User ID, Tour of Duty – Schedule Full Time/Part Time

PII Mapping of Components (Servers/Database)

NCA-Workload and Time Reporting System consists of no key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by NCA-Workload and Time Reporting System 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**
N/A	N/A	N/A	N/A	N/A	N/A

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 information on individuals time and attendance is manually loaded into the tool by the supervisor to track the productivity hours. Files obtained from VATAS, tableau-AMAS and end user time reporting on non-productive time that will be manually uploaded.

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.

VA employees will access the system using single sign on through their PIV. The tool is set up based on role hierarchy and only a supervisor with access to module will be able to login. This tool is a standalone system and data manually extracted from two different systems, VA Time and Attendance System (VATAS) and Automated Monument Application System (AMAS) feed into Tableau is fed into the NCA WATRS.

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

Yes, a report to track production records with employee time availability. Supervisors will be able to actively track employee production against their assigned hours to determine any opportunities or gaps that would allow for additional support to ensure that commitments are made in a timely manner.

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?

As per the role hierarchy, the productivity information of the VA employees is manually uploaded into the tool on a bi-weekly/ weekly basis.

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?

As per the role hierarchy, the productivity information of the VA employees is manually uploaded into the tool on a bi-weekly/ weekly basis.

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.

VATAS data is captured by end user, approved by supervisor and HR manager. End user reporting on the tool for non-productive time is approved by the supervisor. Weekly to bi-weekly the information in the tool will be checked.

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

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

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*

161VA10 Veterans Health Administration Human Capital Management-VA.
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. The authority of maintenance of the system listed in question 1.1 falls under Title 38, United States Code (U.S.C.), Section 501a.

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 basic information of the individual such as name, assigned site location, unique user ID can be used to identify the VA Employee. NCA-WATRS captures the data of the individual to track their productivity and to use the information to report and provide feedback to leadership. The time and availability production report are manually uploaded into a tool on a weekly basis.

<u>Mitigation:</u> Authorization of user to the tool is based on role hierarchy. Only a supervisor/ program manager will have access to all VA Employees productivity profile.

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
First and Last Name	Used as an identifier	N/A
Assigned site location	Used to track the productivity hours and physical locations	N/A
General Schedule (GS) pay scale	Used to trach productivity hours	N/A
Unique user ID	Used as an identifier	N/A
Tour of Duty (full time/part time	Used as an identifier	N/A
Veteran ID	Used to track productivity hours and physical locations	N/A

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?

Salesforce Gov Cloud is used to track the data in the system. Employee time and performance is manually loaded into the Salesforce tool for tracking the productivity of the VA Employees at NCA. The data from the tool will be used for reporting to leadership.

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.

This application reports are more precise, in regards to non-processing time reasons and duration. The application will be considered the individuals performance tracking record through a fiscal year. New records are created each month. The records will be used for award justification and/or performance improvement documentation. The employee will be able to see all of their own records. Only management will be able to see all performance records.

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?

NCA-WATRS system (Salesforce Development Platform) is equipped with the Salesforce Shield Product which provides FIPS 140-2 encryption for 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?

There is no SSN being captured.

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

The only PII would be the employee's name. The system is internal to the division only. Security profiles are in place for each role.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The PII information stored in the NCA-WATRS tool is based on role hierarchy. Only the Supervisor/Program manager with PIV login can access the tool.

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

The PII information stored in the NCA-WATRS tool is based on role hierarchy. Only the supervisor/ program manager with PIV login can access the tool. Only the employee basic information of name against productivity is tracked by the tool.

2.4c Does access require manager approval?

Yes, the supervisor/program manager will approve new users access requests.

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

As per the SORN, the data from the tool will be used for tracking and reporting will be used for performance review board to leadership. This aligns with the tools goal.

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

NCA-WATRS system (Salesforce Development Platform) is equipped with the Salesforce Shield Protect which provides FIPS 140-2 encryption for data in transit and at rest.

The Privacy Officer, Information System Owner, and Information System Security Officer will review users accessing the tool on regular intervals to ensure appropriate access is in place to safeguard the PII.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

NCA-WATRS tool retains the VA Employees information such as First and Last Name, assigned site location, General Schedule (GS) pay scale, Unique User ID, Tour of Duty – Schedule Full Time/Part Time, and Veteran ID.

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.

The performance records will be archived in accordance with records management directives for 3 years.

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?

Yes

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

Records are disposed of in accordance with General Records Schedule (GRS) 5.2, Item 020. Item number: 3075.3, Time and attendance records, disposition authority: GRS 2.4, item 030 DAA-GRS 2019-0004 0002.

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 are electronic, and the details of their disposal will be documented within the SORN. The disposal of SPI should also be recorded as part of the Software as a Service (SaaS) documentation/ contract. The SORN is 161VA10A2/ 83 FR 11297 covers the PII for NCA-WATRS.

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.

NCA-WATRS does not use PII for research, testing or training.

<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:

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 retention risk pertains to the PII information of the individuals being at risk of exposure. There is a risk that unauthorized personnel will attempt to access the data without permission.

Mitigation: To mitigate the risk posed by information retention, NCA-WATRS tool adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500.

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***
National Cemetery Administration	Validate the task completion assigned to specific VA employees	Automated Monument Application System (AMAS)	Manual downloads from AMAS with uploads to NCA WATRS
VA Financial Service Center	Info is used determine employees available business hours.	VA Time and Attendance System (VATAS)	Manual downloads from AMAS with uploads to NCA WATRS

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> There is a potential loss of information due to theft or destruction with the sharing of information. NCA-WATRS is a standalone time reporting system which doesn't connect to other system/ modules.

<u>Mitigation:</u> Every internal system with which NCA-WATRS shares data has an Authorization to Operate (ATO) that describes how PII and PHI are to be protected. Through Continuous Monitoring, data is protected in accordance with the security and privacy controls outlined in their System Security Plans (SSPs) and VA policies and procedures.

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

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a

Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Data contains VA Employees personal information. There is no data externally shared.

Mitigation: No data is externally shared.

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.

Employees are aware their performance data is being collected. They enter non-processing time for approval. Supervisors also conduct monthly performance meetings with each employee. Their performance was collected by user ID from date of hire. No official written notice was provided when moved to a difference platform. The system will be utilized by the supervisors to track the time reporting of individual NCA employee. This will be used for reporting and feedback to leadership only.

161VA10 Veterans Health Administration Human Capital Management-VA Federal Register Privacy Act of 1974; System of Records.

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

Leadership was unaware specific written noticed needed to be provided as VA had already provided notice: https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/05/FY23WorkloadandTimeReportingSystemWATRSPIA.pdf, and the NCA version is not collecting PII.

161VA10 Veterans Health Administration Human Capital Management-VA Federal Register :: Privacy Act of 1974; System of Records

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

Same as above 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.

No, the individual cannot decline the information collected by NCA-WATRS tool. The time reporting of the individual will be utilized to provide feedback to leadership the insight to employees' assignment or hiring.

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.

N/A. The system will be utilized by the supervisors to track the time reporting of individual NCA employee. This will be used for reporting and feedback to leadership only.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: *Has sufficient notice been provided to the individual?*

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: The risk is that individual employees are unaware of the information captured in the NCA WATRS tool for reporting.

Mitigation: Employees are aware of the risk of inputting time tracking in VA systems. Additional mitigation is provided by making the System of Record Notices (SORN) and Privacy Impact Assessment (PIA) available for review online

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.***

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or may write, call or visit the VA facility location where they are or were employed or made contact. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. There is a MPS SOPs for privacy and records management.

Only Supervisors have access to the data. They will be able to actively track employee production against their assigned hours to determine any opportunities or gaps that would allow for additional support to ensure that commitments are made in a timely manner. The system allows data to the employees based on the role hierarchy.

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

The tool 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?

The procedure is the same as 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.

The supervisors have a chance to correct the information uploaded manually to the tool.

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.

Each inaccurate data will be used to match against the VATAS and AMAS tool to validate the information captured for accuracy. The supervisor will also be able to contact the VA employee on issue with their time reporting in case of discrepancy. The correct information can be individually corrected on the tool by the supervisors.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A written email or request can be provided to access the reporting to the NCA-WATRS. Each of these requests will be reviewed by the supervisor.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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?

<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> There is a risk that individuals may seek to access or redress records in the NCA WATRS tool in which they will seek change.

<u>Mitigation:</u> Often, the information to be disclosed to such persons and entities is maintained by Federal agencies and is subject to the Privacy Act (5 U.S.C. 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual.

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?
The manager will review and approve new users.

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?

Contractor support teams possess privileged users responsible for maintaining the system on behalf of the VA. VA role-based security training is required for all privileged users of VA systems. Single sign-on utilizing VA PIV cards and/or Citrix VPN (over contractor laptops and unsecure networks) will be required. Typical privileged users of QMS include:

- Systems Engineer(s) - Privileged Access
- System Administrator(s) – Privileged Access
- Information System Security Engineers (Continuous Monitoring) - Auditor

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.

Managers have create, read, edit, delete access. Team leaders have create, read, and edit. Employees have create and read.

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 Privacy Rules of Behavior Agreement is signed by all VA Contractors who are on-boarded and there is annual engagement to approve. VA contractors working for NCA have to abide by the rules set forth by the VA.

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

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

VA Privacy Rules of Behavior and VA on-boarding enterprise-wide 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:* 02/24/2021
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 06/01/2023
5. *The Authorization Termination Date:* 06/01/2024
6. *The Risk Review Completion Date:* 06/01/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): LOW*

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.***

N/A

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, NCA-WATRS system utilizes Salesforce Gov Cloud. Under the contract: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud.

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 NCA-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 collected by this module.

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, it is, 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).

NCA-WATRS 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.

CYNTHIA MERRITT

Digitally signed by CYNTHIA MERRITT
Date: 2024.03.19 12:06:33 -04'00'

Privacy Officer, Cindy Merritt

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.03.19 13:38:51 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.03.25 10:36:59 -04'00'

Information System Owner, Mike 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).

https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/05/FY23WorkloadandTimeReportingSystemWATRSPIA.pdf, and the NCA version is not collecting PII.

161VA10 Veterans Health Administration Human Capital Management-VA Federal Register :Privacy Act of 1974; System of Records

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