Privacy Impact Assessment for the VA IT System called:

Veterans Tracking Application 2.0 (VTA 2.0)

Veterans Benefits Administration

Veteran Experience Service

Date PIA submitted for review:

10/26/2022

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 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291
Record Officer	Keith Kimmons	Keith.kimmons@va.gov	202-461-9687

Abstract

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

Veterans Tracking Application 2.0 (VTA 2.0) is a Department of Veterans Affairs (VA) solution to streamline and modernize the current VTA application using the Salesforce Platform. VTA 2.0 is developed to support the Integrated Disability Evaluation System (IDES), which is a joint Department of Defense (DoD) and VA disability evaluation process. VTA 2.0 will support VA employees in Veterans Benefits Administration (VBA).

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. *The IT system name and the name of the program office that owns the IT system.*

Veterans Tracking Application 2.0 (VTA 2.0) is controlled by Veteran Experience Service.

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

Veterans Tracking Application 2.0 (VTA 2.0) is a Department of Veterans Affairs (VA) solution to streamline and modernize the current VTA application using the Salesforce Platform. VTA 2.0 is developed to support the Integrated Disability Evaluation System (IDES), which is a joint Department of Defense (DoD) and VA disability evaluation process. VTA 2.0 will support VA employees in Veterans Benefits Administration (VBA).

C. *Indicate the ownership or control of the IT system or project.*

Salesforce Government Cloud Plus (SFGCP) owned in collaboration between Veterans Affairs Central Office (VACO) Information Technology Support Service's (ITSS), Access Management/VA Business Owners and Office of Information Technology (OIT).

2. Information Collection and Sharing

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

The tool is a single office application utilized by 1,980 VA and DOD employee users while serving about 23,286 Veteran applications per year.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

IDES seeks to ensure seamless service delivery by eliminating the duplicate, time-consuming, and often confusing and overlapping elements of the two current disability processes. The IDES seeks to ensure the program provides Soldiers, Sailors, Marines, Airmen and Coast Guardsmen optimal service and satisfaction for them and their family in receiving quality, fair, and just care and benefits.

Wounded, injured and/or ill SMs are entered into IDES based on their Service to see if they meet retention standards. VTA 2.0 tracks these SMs from entrance into IDES through Return to Duty or Separation (with/without benefits). This case management tool, VTA 2.0, will be accessed by VA and DoD employees through Single Sign On (SSO). Employees include Service Member Branch Patient Care Managers/Physicians, DoD Physical Evaluation Board Liaison Officers (PEBLO) and VA Military Services Coordinator (MSC).

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

The tool has two interconnections to VA/ DOD Identity Repository (VADIR) and VBA Data Warehouse (VD2). The VADIR provides Veteran's information to VTA 2.0. This information is then shared with VBA date warehouse (VD2) for reporting purposes.

G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

The tool is a single office application utilized by 1,980 VA and DOD employee users while serving about 23,286 Veteran applications per year. Users are authenticated and allowed access into the tool using Single Sign On (SSO) two-factor authentication. User login and access is monitored to VTA 2.0 tool.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

Although VTA 2.0 data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF Process, the system has a Data Security Categorization of Moderate, with the impacts of a data compromise being identified in the VTA 2.0 Data Security Categorization (DSC) memo. The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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?*

SORN applicable for the system is "Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT) – VA" 163VA005Q3 states the authority for maintaining this system is Title 38 U.S.C. Section 5106. The SORN covers all Personally Identifiable Information (PII) used in VTA 2.0.

D. System Changes

J. Whether 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. Whether the completion of this PIA could potentially result in technology changes

VTA 2.0 is a web-based application. This PIA will not result in any other 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.

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*
☐ 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)

Veteran/ Service Member Electronic Data Interchange Personal Identifier (EDIPI), Compensation and Pension (C&P) such as exam review, exam type, exam provider, exam site, exam review notes. Open text box of notes which may contain additional PHI information not listed in C&P.

PII Mapping of Components (Servers/Database)

Veterans Tracking Application 2.0 consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VTA 2.0 and the reasons for the collection of the PII are in the table below.

Internal Database Connections

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Veterans Affairs Department of Defense Identity Repository (VADIR)	Yes	Yes	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Military Service Information, VA Benefits Information	To properly identify veteran, verify the benefit eligibility and communication regarding benefits	Secure electronic data transfer via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS) and SQL Server Integration Services (SSIS)
Enterprise Data Warehouse (EDW)	Yes	Yes	Name, Social	To properly identify	Secure electronic

			Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Military Service Information, VA Benefits Information	veteran, verify the benefit eligibility and communication regarding benefits	data transfer via SQL Server Integration Services (SSIS)

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?

VTA 2.0 receives data from the VA system VA DOD Identity Repository (VADIR) and data directly from the veteran and dependents to obtain basic demographics and service details for servicemembers from an authoritative source.

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.

Information from VADIR is utilized to validate the service member to receive the qualifying services offered by the Veteran Affairs.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VTA 2.0 is used as the record system which generates reports according to the actively enrolled Service Members into the VA.

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?

VTA 2.0 information is collected through secure data transfer via VADIR web service and verbal input from Veterans and dependents to DOD and VA employee users.

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

There are no forms.

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.

Data is checked for completeness by system audits, manual verifications, and feedback from Veterans.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

VTA 2.0 uses internally developed utilities for checking accuracy, completeness, and validity. Typical rules to determine valid syntax of system inputs consist of character set, length, numerical range, and acceptable values to ensure that inputs match expected format and content criteria. Checks for accuracy, completeness, and validity of information are part of the change management process and Architectural Change & Review Board (ACRB).

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

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

The 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 U.S.C., 5106.

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 PII and PHI information of the service members are at the risk of exposure. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offers assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

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

VTA 2.0 collects information of Veterans data listed below:

- Veteran name/ Service Member (SM) name: used for identifying the Veteran
- Veteran/SM Social Security Number (SSN): Identity SM, search for Cases and pull SM demographics data from VADIR.
- Veteran/SM Electronic Data Interchange Personal Identifier (EDIPI): Identity SM, search for Cases and pull SM demographics data from VADIR
- Veteran/ SM Date of Birth (DOB): used for alternate identification of the Veteran
- Veteran/SM Gender: identification of the gender preference by the Veteran
- Veteran/SM official email address: used for identification and primary contact information
- Veteran/SM personal email address: alternate contact information for the Veteran.
- Veteran/SM Rank: used for validating the rank of active military personnel and for qualifying Veteran benefits
- Veteran/SM Grade: used for validating the grade of active military personnel and for qualifying Veteran benefits
- Veteran/SM Personnel Class: used for validating the class of active military personnel and for qualifying Veteran benefits
- Veteran/SM Military Service: used for validating military personnel service information and for qualifying Veteran benefits
- Veteran/SM Unit: used for validating the unit of active military personnel and qualifying Veteran benefits.
- Veteran/SM Unit Identification Code: used for validating the unit of active military personnel and qualifying Veteran benefits.
- Veteran/SM contact number – home and cell phone number: used for contacting the service member and active Veteran
- Veteran/SM residential and mailing address: used for identifying the residential address of the active military personnel.

- Compensation and Pension (C&P) - exam review, exam type, exam provider, exam site, exam review notes: used for identifying the compensation information of the active military personnel to Veteran eligibility.
- Notes (open text box – may contain additional PHI information not listed in C&P): used for identifying the compensation information of the active military personnel to Veteran eligibility.

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.

VTA uses internally developed utilities for checking accuracy, completeness, and validity. Examples of internally developed utilities include Typical programming rules to determine valid syntax of system inputs consisting of character set, length, numerical range, and acceptable values to ensure that inputs match expected format and content criteria. Checks for accuracy, completeness, and validity of information are part of the change management process and Architectural Change & Review Board (ACR).

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.

The system does save previous cases for an individual member as a part of the archives for the system history. Historical cases may be referenced to support an open case. It will only be referenced, and a new case will be created. Service members can only have one open case at a time. No action will be taken against the individuals for newly derived data other than updates to the personal record in the event data has changed (e.g., name change) Once the new record is created the information is shared with Government employees to document activities during the life cycle of the disability evaluation process. The PEBLO, MSC, PEB Admin, D-RAS, and DES Support team will have access to the case record to modify the fields in the case record based on individual roles.

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?

Data in transit are protected by HTTPS site-to-site encryption. PII data are encrypted at rest with Salesforce Shield encryption.

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

SSN is PII data, encrypted at rest with Salesforce Shield encryption. Additionally, encryption is available based on the business needs.

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

VTA 2.0 system (Salesforce) is an encrypted secure system. User roles in VTA 2.0 determines who has visibility into PII, including SSN.

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 SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran's benefits, such as compensation or education.

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

Yes, Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Yes, 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.

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

IAM systems verify credential and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

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

Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus 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.

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*

VTA 2.0 Salesforce tool retains information of Veterans such as: Veteran name/ Service Member (SM) name, Veteran/SM Social Security Number (SSN), Veteran/SM Electronic Data Interchange Personal Identifier (EDIPI), Veteran/ SM Date of Birth (DOB), Veteran/SM Gender, Veteran/SM official email address, Veteran/SM personal email address, Veteran/SM Rank, Veteran/SM Grade, Veteran/SM Personnel Class, Veteran/SM Military Service, Veteran/SM Unit, Veteran/SM UIC, Veteran/SM contact number – home and cell phone number, Veteran/SM residential and mailing address, Compensation and Pension (C&P) - exam review, exam type, exam provider, exam site, exam review notes, Notes (open text box – may contain additional PHI information not listed in C&P)

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

VHA records are held and destroyed in accordance with varying timetables dependent on the type of data contained in the record outlined in General Records Schedule (GRS) 4.3 (previously GRS 20). An example: Output records are records derived directly from the system master record. Examples include system generated reports (in hardcopy or electronic format), online displays or summary statistical information, or any combination of the above. Temporary; Destroy when business use ceases. Authority: DAA-GRS-2013-0001-0004. VTA information collected that becomes part of the veteran’s electronic health record is retained 75 years after the last episode of care. Additionally, in GRS 4.3 item 010, Hardcopy or analog records previously scheduled as temporary used to create, update, or modify electronic records incorporated in their entirety into an electronic system. (Not media neutral; this applies to hardcopy or analog records only): Destroy immediately after verification of successful conversion, but longer retention is authorized if required for business use. Authority: DAA-GRS-2013-0001-0001.

VBA records are held and destroyed in accordance with Records Control Schedule (RCS) VB-1, Part I and Records Control Schedule (RCS) VB-1, Part II. As an example, VB-1 Part I: Temporary Military File. Correspondence, memoranda, and forms having temporary reference value pertaining to transfer of Veterans' records; mail pertaining to Veterans, their beneficiaries and dependents on matters not administered by VA; Close file after 3 months. Destroy 90 days after close of each quarter.

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?

The retention schedule for the Salesforce Government Cloud Plus (SFGCP) is also applied to VTA 2.0 module.

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. 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). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records)

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

Yes, VBA records are governed by Records Control Schedule (RCS) VB-1, Part II Revised for VBA http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc and by Records Control Schedule (RCS) VB-1, Part I http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc

VHA Records are governed by GRS 4.3 Input Records, Output Records, and Electronic Copies (previously GRS 20) http://www.archives.gov/records-mgmt/grs/grs04-3.pdf

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.

VTA 2.0 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. https://www.va.gov/vapubs/search_action.cfm?dType=1)

.

Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

VTA 2.0 does not use PII information of the users stored in this application for research, testing or training. Users accessing the tool would have to undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually. DOD employees undergo the service/ training prior to accessing the VTA 2.0 application.

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VTA 2.0 could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: Information retained in the system is used for supporting current and former service members through benefits eligibility determination. To mitigate the risk posed by information retention, the VTA 2.0 adheres to the VA RCS schedules for each category or data it maintains. When the retention data is breached for a record, the facility will carefully dispose of the data by the determined method as described in question 3.4. VA Directive 6500 Cybersecurity Program serves as the authoritative source for addressing and managing a cybersecurity breach or attack (also known as a cyber incident) to contain and limit the damage.

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***
VBA Data Warehouse (VD2)/ Enterprise Data Warehouse (EDW)	Provides veteran's primary contact data, military service data, education and benefits data to VTA to support benefits management for severely disabled veterans.	SSN, Benefits Information, Veteran/ Service Member name, DOB, physical/ residential address, contact information (email address and telephone number), Military Service information	Site-to-site encrypted transmission
Veteran Affairs/ Department of Defense Identity Repository (VADIR)	VADIR consolidates data transfers between the DoD and the VA and shares data to VA entities via 12 web services, database to database interfaces, data extracts and reports to assist in determining Veterans' benefits eligibility. VTA 2.0 will utilize the system to capture any new service members that have separated from the armed forms daily.	SSN, Benefits Information, Veteran/ Service Member name, DOB, physical address, contact information (email address and telephone number), Military Service information	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: without appropriate security controls, the PII information shared internally with the system listed is at a risk of unauthorized data access.

Mitigation: Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors. VTA personnel are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system. authenticate external DoD users via CAC (Common Access Card) using VA Single Sign on External (SSOe) and internal VA users via VA SSOi. Encrypted site-to-site transcription. Data and files are encrypted both in transit and at rest. User specific, user access data configured for each role category and on least privilege base.

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***
Department of Defense (DOD)	Eligibility/ Benefits	Name, SSN, DOB, Mailing address, zip code, phone numbers, email address, military service information, VA benefits information	SORN 163VA005Q3 Memorandum of Understanding (MOU)/ Interconnection Security Agreement (ISA)	CAC authentication

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.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized VA program, system, or individuals

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

Section 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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1. The SORNs defines the information collected from Veterans, use of the information, and how the information is accessed and stored. Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT)-VA 163VA005Q3.(https://www.govinfo.gov/content/pkg/FR-2021-04-30/pdf/2021-09084.pdf)
2. This Privacy Impact Assessment (PIA) also serves as notice of the Veterans Tracking Application 2.0. 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 provided via VA Privacy Policy

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.

Service members (or designated representative) once enrolled in the IDES program are counseled upon enrollment into the IDES program. Veterans complete the VA 21-22 (series) which is governed by OMB Control No. 2900-032, Section 2 of VA Form 21-0819 DoD Referral to Integrated Disability Evaluation System and DD Form 2807-1 "Report of Medical History" to inform those affected of their protection by sections 5101, 5701, 7332, Title 38, U.S.C.

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.

Veterans and Service members may refuse to provide information, but it may impact the determination of benefits.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

Veterans and Service members may refuse to provide information, but it may impact the determination of benefits.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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>: Risk is associated with members of the public/ Veterans being unaware their VTA 2.0 system exists within the Department of Veterans Affairs.

<u>Mitigation</u>: The VA mitigates this risk by providing the public with notice that the system exists, as discussed in detail in question 6.1, included in the System of Record Notice.

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 a record pertaining to them on VTA 2.0 system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notices. Contact the system manager, in writing, and send it to Delwin Johnson, Product Line Manager (VTA), Office of Information & Technology, Department of Veterans Affairs, 810 Vermont Ave. NW, Washington, DC 20420. Requests should contain the full name, address and telephone number of the individual making the inquiry.

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).

System 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.

Not applicable for the system.

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.

Veterans have the right to amend their records by submitting their request in writing with a wet signature. As stated in SORN, 163VA005Q3, Veterans Tracking Application (VTA)/ Federal Case Management Tool (FCMT)-VA Individuals seeking information on the existence and content of a record pertaining to them should contact the system manager, in writing, at the address listed in 7.1. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Individuals are notified in two ways the publishing of the SORN and publishing of this document. As stated in SORN, Veterans Tracking Application (VTA)–VA'' (163VA005Q3), Federal Case Management Tool (FCMT)-VA Individuals seeking information on the existence and content of a record pertaining to them should contact the system manager, in writing, at the above address (listed in section 7.1 and 7.2).

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.

Formal redress is provided in the SORN. As stated in SORN, 163VA005Q3, Veterans Tracking Application (VTA)–VA/ Federal Case Management Tool (FCMT)-VA. Individuals seeking to contest the content of a record pertaining to them should contact the system manager, in writing, at the above address (listed in section 7.1 and 7.2). Requests must be made in writing with a wet signature.

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>: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

<u>Mitigation</u>: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of application. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about application.

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.

Per VA Directive 6500, the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

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?

The VA documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of TMS.

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.

Role-based hierarchy is set up for user access. Profiles and permission sets are applied to the users accessing the platform. VTA authentication is a two-step process which involves the cooperation of a user’s supervisor and the VTA help desk. The end will begin the process by submitting a VTA registration request. A request will be generated to their supervisor. The supervisor will approve their request. The request will be forwarded to the VA admin for approval. After registering for a VTA account, a message is sent to the VTA Help Desk who will give the final access controls and authorization to the user. IAM handles authentication while VTA handles authorization. VTA can enable or disable VTA access and provide all roles that are associated with accounts. Users are accountable for actions performed with their user ID and will be held liable for actions determined to be intentionally malicious, grossly negligent, or illegal. Users are authenticated by PIV (SSOi) for VA users while DOD users are authenticated via (Common Access Card) using VA SSOe.

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 access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are 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 TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

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. General Training includes VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-Boarding enterprise-wide training. After the user’s initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

Please provide response here

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, VTA 2.0 utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*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 shared through the VTA 2.0. 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.

Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in the VTA 2.0 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.

VA has full authority over data stored in Veterans Tracking Application 2.0 (VTA 2.0).

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).

VTA 2.0 does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

LAKISHA V WRIGHT 111646

Digitally signed by LAKISHA V WRIGHT 111646
Date: 2022.11.01 09:04:51 -04'00'

Privacy Officer, Lakisha Wright

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.11.01 12:49:26 -04'00'

Information System Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.11.01 11:02:55 -04'00'

Information System Owner, Michael Domanski

Keith H. Kimmons 1717335

Digitally signed by Keith H. Kimmons 1717335
Date: 2022.11.01 09:30:19 -04'00'

Records Management Officer, Keith Kimmons

APPENDIX A-6.1

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

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

Federal Regulation: 38 CFR 1.579.

31 CFR § 1.32 - Use and disclosure of social security

Notice provided via VA Privacy Policy

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

VB-1, Part II Revised for VBA:
http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc

Records Control Schedule (RCS) VB-1, Part I:
http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc

VHA Records: Input Records, Output Records, and Electronic Copies

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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