Privacy Impact Assessment for the VA IT System called:

Salesforce - VA Monthly Stipends Training Program (NVSPSE Stipends4Vets)

Veterans Health Administration

National Veterans Sports Programs and Events (NVSPE)

eMASS ID: 1907

Date PIA submitted for review:

04/03/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	James Boring	James.boring@va.com	215-842-2000 ext 4613
Information System Owner	Michael Domanski	Michael.domanski@va.com	727-595-7291

Abstract

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

The Salesforce – VA Monthly Stipend Training Program (National Veteran Sports Programs & Special Events (NVSPSE Stipends) (Stipends4Vets) is a module that allows Veteran Olympic & Paralympic Athletes to apply for and request monthly stipend payments to support their training and participation in related activities for their sport. The Stipends4Vets module has three key types of users, all of whom will be accessing the module to create & review data to perform their roles in the process:

- Veteran Athletes will register as a user through accessing a dedicated Salesforce Experience Site for Veterans. Veteran Athletes will only have access to their own data related to the program.

- External Governing Body officials will review and approve that the athletes meet the standards of the program. These officials will register for and be approved to access a dedicated Salesforce Experience Site for Certifying Officials. Certifying Officials will only have access to submitted data from the Veteran Athlete that is associated with their Governing Body (e.g. USA Archery) and relevant to their role in the approval process.

- VA Staff will manage and review the information provided and subsequently enter it into systems to process the stipend payment to the Veteran Athlete. These staff members will use a dedicated Salesforce app for the Stipends4Vets program. The data elements which are sent to the FSC to issue payment are listed in this systems Data Security Categorization document: The VA-FSC vendor file request form includes: VA facility information, Payee/Vendor Information, Station number, Commercial vendor, Registered in SAM.gov, Station phone number, Station fax number, Station email address, DUNS number, DUNS+4, SSN/TIN, NPI, Payee/vendor name, DBA, Contact Email address, Phone number, Current address, Previous address, Bank name, Bank address, Nine-digit bank routing number, Account number, Account type, Name and title of Payee/vendor, and Signature of Payee/Vendor.

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 - VA Monthly Stipends Training Program (NVSPSE Stipends) is a VA-owned Salesforce-controlled system built on the Salesforce Government Cloud Plus (SFGCP) for the National Veterans Sports Programs and Special Events Office.

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

Stipends4Vets is a module that allows Veteran Olympic & Paralympic Athletes to apply for and request monthly stipend payments to support their training and participation in

related activities for their sport.

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

Stipends4Vets is a VA-owned Salesforce-controlled system built on the Salesforce Government Cloud Plus (SFGCP) for the National Veterans Sports Programs and Special Events Office.

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?

In total there will be about 4,500 users using this solution. The module will allow Veterans to track the progress of their application throughout the review and decision process.

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

The Stipends4Vets module allow veterans to track the progress of their application throughout the review and decision process. There are three key types of users: Veteran Athletes, External Government Body Officials, and VA Staffs, all of whom will be accessing the module to create & review data to perform their roles in the process.

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 five internal connections: Master Person Index (MPI), ID.me, DS Logon, VA My HealtheVet, and VA Profile and an additional data element is being stored for Veteran Status. Veterans will use a VA.gov website link to access Veteran Community, The Veteran Community will provide a redirect to AccessVA IAM site. Users will authenticate if they have not been authenticated already in VA.gov. Upon successful authentication, the SAML assertion generated by AccessVA IAM will allow access to Veterans Stipends4Vets Salesforce community. No external connections to this application.

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?

This system is only used by the VA National Veterans Sports Programs & Special Events Office, which is lead and managed by VA employees; every employee receives annual training on how to protect PII no matter the location.

3. Legal Authority and SORN

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

Stipends4Vets 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 Stipends4Vets Data Security Categorization (DSC) memo. The Privacy Act is the legal authority to utilize this information.

The Privacy Act is the legal authority to utilize this information. 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, *79VA10 / 85 FR 84114, "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA"*. The SORN specifies that information may be used to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics). AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

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?*

The SORN is not required to be updated. The cloud usage and storage for the system is covered under this SORN.

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 result in no business process changes within this solution.

K. *Will the completion of this PIA could potentially result in technology changes?*

The completion of this PIA will result in no technological changes within this solution.

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)

Other PII/PHI data elements: Veteran Status, Healthcare Eligibility Status, Business Email Address.

PII Mapping of Components (Servers/Database)

VA Monthly Stipends Training Program (NVSPSE Stipends) consists of 5 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA Monthly Stipends Training Program (NVSPSE Stipends) 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**
VA Identify and Services Master Person Index (MPI)	Yes	Yes	First Name, Last Name, Social Security Number, Date of Birth, Address, Email, ICN (Internal	Veteran identification verification	VA Identity and Access Management Programs and mandatory

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

			Control Number), Gender, Phone Number.		annual Privacy, HIPAA, and information security training.
ID.ME	Yes	Yes	First name, Last Name, Email address	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.
DS Logon	Yes	Yes	First name, Last Name, Email address	Veteran identification verification	DoD and VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.
My HealtheVet	Yes	Yes	First name, Last Name, Email address	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.
VA Profile	Yes	Yes	Healthcare eligibility Status	Veteran identification verification	VA Identity and Access Management Programs and

					mandatory annual Privacy, HIPAA, and information security training.

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 source of information is provided directly from the veterans who inputs the data on Stipend4Vets portal.

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

This question is not applicable for the tool. The information is only collected from the individual.

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

This is not applicable because the system does not create information; it simply aggregates it.

1.3 How is the information collected?

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

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

The information is collected directly from the Veterans who enters their information into the Stipends4Vets online web platform.

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?

No paper will be generated from the information collected on the registration forms. The program and event registration forms are online webforms that save information directly into the Stipends4Vets Module.

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.

Information in the Master Person Index (MPI) is managed by the respective VA unit. This will be utilized to validate the information the Veteran provides on Stipends4Vets. Stipends4Vets is a read-only consumer of this data and additional system checks for accuracy are not performed.

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?

Same as above, refer to 1.4a.

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

Authority to collect and maintain the information is found in the Privacy Act System of Record Notice (SORN) 79VA10 / 85 FR 84114 "Veterans Health Information Systems and Technology Architecture (VistA) records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdfAuthority for maintenance of the system: Title 38, United States Code, section 7301(a).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information (SPI) including personal contact information, SSN and disability rating may be released to unauthorized individuals.

Mitigation: Profile based permissions will govern what access users have access to. The profiles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

Privacy Risk: Unsecured Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be exposed.

Mitigation: To mitigate this risk, the Stipends4Vets Application protects data by ensuring that only authorized users can access it. Data security rules are assigned that determine which data users can access. All data is encrypted in transfer. Access is governed by strict password security policies. All passwords are stored in Secure Hash Algorithm (SHA) 256 one-way hash format.

Privacy Risk: Data breach at the facilities level.

Mitigation: To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the salesforce system rooms/cages. All buildings are completely anonymous, with bullet---resistant exterior walls and embassy---grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

Privacy Risk: Data breach at the network level.

Mitigation: Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on specific ports, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two---factor authentication, along with the extensive use of technology that controls points of entry.

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
Name	Use to identify veterans	N/A
Social Security Number	Use to identify veterans	N/A
Date of Birth	Used to identify Veteran's age	N/A
Gender	Demographic Information	N/A
Phone Number	Used for communication	N/A
ICN (Internal Control Number)	Use to identify veterans	N/A
Healthcare eligibility Status	Use to verify eligibility	N/A
Veteran Status	Use to identify veteran status	N/A
Personal Email address	Used for communication	N/A
Mailing Address	Uses for mandatory funding reporting	N/A
Financial Information	Payment processing	N/A
Tax Identification Number	Payment processing	N/A
Service Connection	Use to verify eligibility	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?

Stipends4Vets does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

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 not create or make available new or previously unutilized information about an individual. It is used to run reports.

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?

The tool utilizes Salesforce Shield protect adhering to FIPS 140-2 encrypted connection. Platform encryption using Salesforce shield to protect data-at-rest.

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

Same as above 2.3a.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. Personnel 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.

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?

Access to PII/PHI is determined by whether a user is a member of the NVSPSE program office that is working on this system. Since no PII/PHI is shared externally a user must be a member of this office to have access.

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

Users must be approved by the business owner and provision by the Digital Transformation Center. To receive access to the SFGCP Platform, user of the SFGCP with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level contract of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center. The Digital Transformation Center team also has read/write access to the Stipends4Vets Applications, as administrators of the VA Salesforce system.

2.4c Does access require manager approval?

New users will be provided access to the tool by managerial approval process.

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

Yes, employees accessing the record of the veterans are monitored, tracked, and recorded.

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

All VA employees working with the NVSPSE program, interacting with Veteran records are responsible for safeguarding PII. Information collected will only be used for event planning, execution and reporting metrics as required by VA leadership.

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*

- First Name
- Last Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Veteran Status
- Gender
- Phone Number
- Healthcare eligibility Status
- ICN (Internal Control Number)
- Personal Email address
- Mailing Address
- Financial Information
- Tax Identification Number
- Service Connection

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.

Retention of Records is expected to be 75 years. 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.pd

The SORN provides the retention information as Record Control Schedule (RCS) 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS 10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

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?

Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period, which could be as much as 75 years. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to Record Control Schedule 10-1. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

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

Same as above, 3.3a.

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.

Active Data stays on disk until the VA deletes or changes it. Data on backups is retained for 90 days until the backups are overwritten. Log data is retained by Salesforce for a year. VA exports data and retains it to meet VA/NARA retention requirements and dispose of the exported data at the end of the retention period. When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard

drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below. Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce's control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce's Media Handling Process. All data is handled and located in VA own Salesforce's servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center facilities until onsite media destruction takes place. Leasing equipment provides salesforce the opportunity to use the latest equipment available from vendors. Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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: Veterans' information is listed in the system. The risk is associate with longer retention of veteran information stored or retained by NVSPSE Stipends4Vets.

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Veterans Health Administration (VHA)	To validate the individual/Veteran registering for an event	First Name, Last Name, Social Security Number, Date of Birth, Address, Email, ICN (Internal Control Number), Gender, Phone Number	Data is provided via the AccessVA SAML response when authenticating a user
Health Eligibility Center (HEC)	To verify healthcare eligibility	First Name, Last Name, Social Security Number, Date of Birth	Data is provided via the AccessVA SAML response when authenticating a user

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: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: 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.

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***	***List the method of transmission and the measures in place to secure data***

			be more than one)	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: No data is shared with any parties external to VA.
There is a privacy risk in collecting veterans information used for NVSPSE events. If this information were released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to those individuals.

Mitigation: Identify access management controls are in place and contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. Personnel 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.

Section 6. Notice

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

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

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

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

Yes, individuals are provided Privacy Notices for this system in multiple ways.

1) The SORN that applies to this system, 79VA10 identifies the information collected from Veterans, use of the information, and how the information is accessed and stored.

2) This Privacy Impact Assessment will also be made available to the public to view and will serve as a notice. 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." It can be found at this website: https://www.oprm.va.gov/privacy/pia.asp.

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

A notice is provided.

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.

A paragraph on the homepage of the Sports4Vets community informs the Veteran of the privacy policy with the above weblink. The paragraph states:

The National Veterans Sports Program & Special Events (NVSPSE) is committed to providing the best possible care to our veterans. Information we gather from your interaction with our website and the services you access through our website, help us better understand and serve your needs during event planning and execution. We only collect personal information that you provide to us. Please take a moment to review our privacy, policies and legal information page.

In addition, when a Veteran completes a registration form, the weblink to the privacy policy will be under the submit button with the statement "By clicking Submit, you agree to the VA's privacy policy.

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.

Yes, if a Veteran refuses to provide information suitable for a Stipends4Vets application and stipend request they will not receive a stipend payment.

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.

No

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: There is a risk that Veterans will not know that applications built on the SFDP collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The VA mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1, including the SORN and the Privacy Act Statement.

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 may submit a FOIA request by visiting www.foia.gov; then searching for the Department of Veterans Affairs, and then navigating to the Veterans Health Administration (VHA) and following the prompts. An alternate method would be to send an email to the VHA FOIA Public Liaison at vhafoiahelp@va.gov, or by calling +1 (833) 880-8500.

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 system is not exempt from the 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?

N/A – The system is a Privacy Act 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.

Information on the user's account is sourced from the MPIe, ID.me, My HealtheVet, and DS Logon. These source systems are responsible for maintaining the user's data. Should an update be needed to any of the information sourced from these systems, the Veteran may contact the Stipends4Vets help desk which will facilitate notifying the system owners with needed correct.

Every page of the Stipends4Vets application the Veteran has access to an active support line (M-F 9am-5pm ET) where they can reach live representatives and follow the procedure to correct their information. Veterans are direct to update their info at: https://www.va.gov/resources/change-your-address-on-file-with-va/

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.

Every page of the Stipends4Vets Application the Veteran has access to an active support line where they can reach live representatives and follow the procedure to correct their information. The Veteran has access to a VA employee where they can reach someone from the event staff and follow the procedure to correct their information. Notification for correcting the information must be accomplished by informing the individual to whom the record pertains to by mail. The individual requesting the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was

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

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***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.

Stipends4Vets users can update preference information on the Veteran's behalf. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the information they are now providing supersedes that previously provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Veterans names, emails, address and phone numbers are listed within the system

Mitigation: Only VA staff and national governing body staff part of the organization the Veteran participate with can see the Veteran information.

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?

User roles are NVSPSE Program Specialist, ALAC Technical Accountant. Both have Read/Write to Stipend Applications & Stipend Requests and their roles identify the information and applications a user can access. The distinction between the roles is controlled by Permission Set assignments. In order to receive these permissions and gain access to records with Veteran and Stipend Application/Stipend Request information, users must be approved by the business owner and then provisioned by the Digital Transformation Center. To receive access to the SFDP, another user of the SFDP with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level contract of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center. The Digital Transformation Center team also has read/write access to the Stipend Applications and Stipend Requests, as administrators of the VA Salesforce system. These users will not be regularly accessing or modifying these records unless their assistance is directly requested by the NVSPSE Director's Office/business owner.

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?

N/A – There are no other agency users.

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.

Director Level staff are able to Read/Write all data for Stipends4Vets Applications & Requests. Certifying Officials are able to Read/Write only information that is pertinent to them reviewing the data about a Veteran training status and position on the national team, for example this level of access is not able to view dependent information or view a Veterans SSN in the contact record. The distinction between the roles is controlled by Permission Set assignments.

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.

The contractors who provide support to the system (monitoring the support line, answering questions on how to interact with the system, assistance with login access) are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts. Contractually all contractors are required to sign the VA Form 0752 NDA.

System Owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform 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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/8/2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 07/11/2023
5. *The Authorization Termination Date:* 07/11/2026
6. *The Risk Review Completion Date:* 07/11/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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. This software application utilizes the Salesforce Government Cloud Plus Platform-as-a-Service (PaaS), which is built on the underlying Salesforce.com that is hosted in a FedRAMP-certified FISMA-High environment, which is in the Amazon Web Services (AWS) GovCloud West 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 shared through the Registration4Vets platform. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.

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.

The VA has the ownership over the ancillary data. The CSP (Cloud Service Provider) does not collect ancillary data.

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.

Details covered in the contract: VA Enterprise Case Management (VECMS) Salesforce Development (Service Provider: Salesforce, Contract Number: GS-35F-0287P Order Number: GS00Q16AEA10013610B18F2981).

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).

The system does not utilize Robotics Process Automation (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.

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.09.18 14:55:10 -04'00'

Privacy Officer, Dennis Lahl

JAMES BORING Digitally signed by JAMES BORING
Date: 2024.09.26 13:22:45 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2024.09.26 11:25:23 -04'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

https://www.oprm.va.gov/privacy/pia.asp.

SORN 79VA10 / 85 FR 84114, "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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