Privacy Impact Assessment for the VA IT System called:

Salesforce: NVSPSE Registration4Vets

Veterans Health Administration

National Veterans Sports Programs and Special Events (NVSPSE) Office

eMASS ID# 2008

Date PIA submitted for review:

12/04/2024

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.gov*	*215-842- 2000 Ext: 4613*
Information System Owner	*Michael Domanski*	*michael.domanski@va.gov*	*727-595-729*

Abstract

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

Salesforce - NVSPSE Registration4Vets will replace current paper/manual processes and various online processes with a single online platform that Veterans can use to sign up for National Veterans Sports Programs and Special Events (NVSPSE) national rehabilitation events. The module will record how many Veterans apply to take part in an event, how many are accepted into the event, how many Veterans attend the event, and various aspects related to the event. The module will allow Veterans to track the progress of their application through the review and decision process. NVSPE is using Box to create, share, and collaborate on training files that are being created for their staff. Box will assist in managing large data files for the events ensuring accurate collection and management of NVSPSE program's data.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

It tracks how many veterans are accepted into the event, how many Veterans attend the event, and various aspects related to the event. This solution will replace current paper/manual and various online processes with a single online platform which Veterans can use to sign up for National Veterans Sports Programs and Special Events (NVSPSE) national rehabilitation events.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

Registration4Vets 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

C. Indicate the expected number of individuals whose information is stored in the system and include 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.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☒	Members of the Public/Individuals
☒	Volunteers

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

Registration4Vets will replace current paper/manual and various online processes with a single online platform which Veterans can use to sign up for National Veterans Sports Programs and Special Events (NVSPSE) national rehabilitation events. The module will record how many Veterans apply to take part in an event, how many are accepted into the event, how many Veterans attend the event, and various aspects related to the event. The module will allow Veterans to track the progress of their application through the review and decision process.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

The tool has five internal connections: Master Person Index (MPI), ID.Me, DS Logon, VA My HealtheVet, VA Profile, and Access VA 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 Registration4Vets Salesforce community. No external connections to this application.

F. Are the modules/subsystems only applicable if information is shared?

Yes, the modules/subsystems are applicable because the system receives, stores, or shares data with the component/modules/subsystems.

G. Is the system operated in more than one site to include primary and secondary 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?

No. NVSPSE Registration4Vets is considered a single site controlled by VA Employee internal users only. It is hosted in the Salesforce Government Cloud Plus, which relies on the Amazon Web Services (AWS) infrastructure.

3. Legal Authority and System of Record Notices (SORN)

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

Registration4Vets 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 Registration4Vets Data Security Categorization (DSC) memo.
Privacy Act System of Record Notice 79VA10 "'Veterans Health Information Systems and Technology Architecture (VistA) Records-VA" is the legal authority to utilize this information. 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 is Title 38, United States Code, section 7301(a).

H. What is the SORN?

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.

I. SORN revisions/modification

Currently there are no requirements for a SORN revision/modification.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No, the SORN require amendment or revision and approval.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

K. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

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 Information 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
- ☒ **Full** Social Security Number
- ☐ **Partial** 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/Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal

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

Identifier (EDIPI) ☒
Other Data Elements (list below)

Other PII/PHI data elements: VA Member ID, Age, Primary Disability/diagnosis/Type of Injury, Patient Require Attendant, Uses of Adaptive Equipment, Details of Adaptive Equipment, Medical History, Known Allergies, Date of last Tetanus Shot, Needs a Sharps Container, Taking Coumadin, Taking Other Anticoagulant/List, Does Patient Smoke, Alcohol or Other Substance Abuse/Explanation, Height, Weight, Pulse, Cardiac, Blood Pressure, Head & Neck, Pulmonary, Abdomen, Skin, Extremities, HEENT, Neuro, Cardiopulmonary review of systems was done and is unremarkable, Detailed Neuro Findings - Manual Muscle, Test, Other finding, Is Medically and Behaviorally Fit to Participate, VAMC where patient receives care, Is Patient Legally Blind, Description of Remaining Vision, Patient's, Level of Independence, Uses Wheelchair majority of time, Will patient need to ski sitting down, Sitting Balance, History of Altitude Sickness/Explanation, Patient have Dysreflexia/Explanation, Oxygen Requirements/Explanation, COVID Fully Vaccinated, Patient on Dialysis, Patient on a, Ventilator, Disability Percentage, Veteran Status, History & Physical problem list with Medical & Surgical History, Recent EKG for any patient 40 or older, Discharge Summary if hospitalized for the last three years, Preferred Language, Service-Connected disability, and percentage, Branch of Service, Time Served, Current Active Duty, and Religion, Volunteer First name, Volunteer Last name, Volunteer Email, Volunteer Phone Number, QR Scan (Pulls the veteran's Bib Number, First name, Last name), and Mobile Data Entry, Pronouns, Sexual Orientation, Religion, Age.

1.2 List 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 Registration4Vets 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.

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?

No, the system does not create information; it simply aggregates it.

1.3 Methods of information collection
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 Registration4Vets 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 form will be generated from the information collected on the registration forms. The program and event registration forms are online web forms that save information directly into the Registration4Vets Module.

1.4 Information checks for accuracy, and 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 provide on Registration4Vets. Registration4Vet is a read-only consumer of this data and additional system checks for accuracy are not performed. Based on the frequency of the Veterans registration into the tool.

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?

Information in the Master Person Index (MPI) is managed by the respective VA unit. This will be utilized to validate the information the Veteran provide on Registration4Vets. Registration4Vet is a read-only consumer of this data and additional system checks for accuracy are not performed. Based on the frequency of the Veterans registration into the tool.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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.pdf.
Authority 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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: 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: The data is secure by Salesforce Shield protect which utilizes FIPS 140-2 encrypted connection.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
First Name	Identification of the veterans to register for NVSPSE programs	N/A
Last Name	Identification of the veterans to register for NVSPSE programs	N/A
Email	Identify veteran and used for communication with veteran on rehabilitation programs	N/A
Phone Number	Identify veteran and used for communication with veteran on rehabilitation programs	N/A
Pronouns	Identification of the veterans to register for NVSPSE programs	N/A
Sexual Orientation	Identification of the veterans to register for NVSPSE programs	N/A
Gender Identity	Identification of the veterans to register for NVSPSE programs	N/A
Gender	Identification of the veterans to register for NVSPSE programs	N/A
Home Address	Identify veteran and used for communication with veteran on rehabilitation programs	N/A
Religion	Identification of the veterans to register for NVSPSE programs	N/A
Medical Information (To Disclose Injury)	Identification of the veterans to register for NVSPSE programs	N/A
Social Security Number	Identification of the veterans to register for NVSPSE programs	N/A
Emergency Contact	To reach out to individual information provided by the veteran for emergencies	N/A
Preferred Language	Identification of the veterans to register for NVSPSE programs	N/A
Service-Connected disability, and percentage	Identification of the veterans to register for NVSPSE programs	N/A
Branch of Service	Identification of the veterans to register for NVSPSE programs	N/A
Time Served	Identification of the veterans to register for NVSPSE programs	N/A
Current Active Duty	Identification of the veterans to register for NVSPSE programs	N/A
Date of Birth Age	Identification of the veterans to register for NVSPSE programs	N/A

VA member ID	Identification of the veterans to register for NVSPSE programs	N/A
Patient Require Attendant	Helps event staff determine food/lodging and other logistical requirements	N/A
Uses of Adaptive Equipment	Helps event staff determine logistical requirements	N/A
Details of Adaptive Equipment	Helps event staff determine logistical requirements	N/A
Medical History	Identification of the veterans to register for NVSPSE programs	N/A
Height and Weight	Helps determine if a Veteran can safely participate in an event	N/A
Head & Neck	Helps determine if a Veteran can safely participate in an event	N/A
Pulmonary, Abdomen, Skin, Extremities	Helps determine if a Veteran can safely participate in an event	N/A
Head, Ears, Eyes, Nose, and Throat examination	Helps determine if a Veteran can safely participate in an event	N/A
Cardiopulmonary review of systems was done and is unremarkable	Helps determine if a Veteran can safely participate in an event	N/A
Neuro	Helps determine if a Veteran can safely participate in an event	N/A
Detailed Neuro Findings - Manual Muscle, Test	Helps determine if a Veteran can safely participate in an event	N/A
Other finding	Helps determine if a Veteran can safely participate in an event	N/A
Is Medically and Behaviorally Fit to Participate	Helps determine if a Veteran can safely participate in an event	N/A
VAMC where patient receives care	Helps determine if a Veteran can safely participate in an event	N/A
Is Patient Legally Blind	Helps determine if a Veteran can safely participate in an event	N/A
Description of Remaining Vision	Helps event staff determine logistical requirements	N/A

Patient's Level of Independence	Helps event staff determine logistical requirements	N/A
Uses Wheelchair majority of time	Helps event staff determine logistical requirements	N/A
Will patient need to ski sitting down	Helps event staff determine logistical requirements	N/A
Sitting Balance	Helps event staff determine logistical requirements	N/A
History of Altitude Sickness/Explanation	Helps determine if a Veteran can safely participate in an event	N/A
Patient has Dysreflexia/Explanation	Helps determine if a Veteran can safely participate in an event	N/A
Oxygen Requirements/Explanation	Helps determine if a Veteran can safely participate in an event	N/A
COVID Fully Vaccinated	VA regulation for participation	N/A
List of Current Medications	VA regulation for participation	N/A
Patient on Dialysis	Helps determine if a Veteran can safely participate in an event as well as logistical requirements	N/A
Patient on a Ventilator	Helps determine if a Veteran can safely participate in an event as well as logistical requirements	N/A
Disability Percentage	Determine eligibility for event	N/A
History & Physical problem list with Medical & Surgical History	Helps determine if a Veteran can safely participate in an event	N/A
Recent EKG for any patient 40 or older	Helps determine if a Veteran can safely participate in an event	N/A
Discharge Summary if hospitalized for the last three years	Helps determine if a Veteran can safely participate in an event	N/A
ICN (Internal Control Number)	Identification of the veterans to register for NVSPSE programs	N/A
Healthcare eligibility Status	Help verify veteran benefit eligibility	N/A
Veteran Status	Identification of the veterans to register for NVSPSE programs	N/A
Volunteer First Name	Identification of the volunteers to assist with registering veterans for NVSPSE programs	N/A

Volunteer Last Name	Identification of the volunteers to assist with registering veterans for NVSPSE programs	N/A
Volunteer Email	Identification of the volunteers to assist with registering veterans for NVSPSE programs	N/A
Volunteer Phone Number	Identification of the volunteers to assist with registering veterans for NVSPSE programs	N/A
QR Scan (Pulls the veteran's Bib Number, First Name, Last name)	Identification of the veterans to register for NVSPSE programs	N/A
Mobile Data Entry	Identification of the veterans to register for NVSPSE programs	N/A

2.2 Describe the types of tools 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?

Cloud computing is used to help analyze the data, in addition a web portal is utilized for Veterans to upload their information. Based on the information provided the Veteran, this tool creates data gathering on the participant registered to the event, selected participants for the events and the events. Data is used for reporting general event activities and planning such as, hotel booking, t-shirt ordering.

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.

A Veteran who chooses to participate in one or more of the NVSPSE sponsored events will voluntarily provide information that will be used in all events on a profile registration form and then will subsequently provide event specific information on event specific registration forms. Both forms will contain some PII and PHI information. Within Salesforce, the profile registration form will create a new Registrant record to store this data. When the Veteran completes an event specific registration form, a new event specific registration application will be created to store the data. When the Veteran completes the forms, they will receive an email confirming the registration. NVSPSE staff will then use this information to plan, execute and report on the specific event the Veteran has

signed up for. Data collected will determine eligibility to participate in the event (eg medical suitability, event capacity limits, qualifying diagnoses)

2.3 How the information in the system is 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? (refer to PTA question 3.8).

Registration4Vets module will only collect the last 4 digits. Salesforce Shield Protect, which provides FIPS 140-2 Certified Encryption. Data in transit and at rest are also encrypted.

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? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

To receive these permissions and gain access to records with Veteran and Registration4Vets Application/Registration4Vets Request information, users must be approved by the business owner and then provisioned by the Digital Transformation Center (DTC). To receive access to the Salesforce Government Cloud Plus (SFGCP) platform, another 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 DTC. The DTC team also has read/write access to the Registration4Vets Applications and Registration4Vets Requests, as administrators of the VA Salesforce system.

2.4c Does access require manager approval?

Yes

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

Yes

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Registrations4Vets is accessed via a secured webpage utilizing SSO technology. Registrations4Vets is housed in a vendor-owned AWS GovCloud Plus, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.

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

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*

All information entered by the Veteran into the Registration4Vets portal is retained: SSN (last 4), VA Member ID, Address, Email Address, Date of Birth or Age, Primary Disability/diagnosis/Type of Injury, Patient Require Attendant, Uses of Adaptive Equipment, Details of Adaptive Equipment, Medical History, List of Medications, Known Allergies, Date of last Tetanus Shot, Needs a Sharps Container, Taking Coumadin, Taking Other Anticoagulant/List, Does Patient Smoke, Alcohol or Other Substance Abuse/Explanation, Height, Weight, Pulse, Cardiac, Blood Pressure, Head & Neck, Pulmonary, Abdomen, Skin, Extremities, Neuro, Cardiopulmonary review of systems was done and is unremarkable, Detailed Neuro Findings - Manual Muscle, Test, Other finding, Is Medically and Behaviorally Fit to Participate, Patient's Daytime Phone Number, Patient Cell Number, VAMC where patient receives care, Is Patient Legally Blind, Description of Remaining Vision, Patient's, Level of Independence, Uses Wheelchair majority of time, Will patient need to ski sitting down, Sitting Balance, History of Altitude Sickness/Explanation, Patient have Dysreflexia/Explanation, Oxygen Requirements/Explanation, COVID Fully Vaccinated, List of Current Medications, Patient on Dialysis, Patient on a Ventilator, Disability Percentage, History & Physical problem list with Medical & Surgical History, Recent EKG for any patient 40 or older, Discharge Summary if hospitalized for the last three years, Veteran Full Name, Pronouns, Sexual Orientation, Gender Identity, Religion, Emergency Contact, Preferred Language, Service-Connected disability, and percentage, Branch of Service, Time Served, Current Active Duty, and Veteran Status.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The information is retained following the policies and schedules of VA's Records Management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

The 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 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes. All records are stored within the system of record indicated on an approved disposition authority.

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

3.4 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 PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans' Affairs VA Directive 6500 (January 24, 2019), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf).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.

No, Registration4Vets does not use live PII information of the veterans 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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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 and NVSPSE events are listed in the system. The risk is associate with longer retention of veteran information stored or retained by NVSPSE Registration4Vets.

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.

PII Mapping of Components

4.1a Registrations4Vets consists of 6 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 Registrations4Vets 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 3.9a 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	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy,

			Birth, Address, Email, ICN (Internal Control Number), Gender, Phone Number.		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.
Access VA	Yes	Yes	First Name, Last Name, Phone Number, Email Address	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***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 VA network 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 in 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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: There is no external sharing.

Mitigation: There is no external sharing.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

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

1) The registration site contains the following statement and link: The National Veterans Sports Programs & Special Events (NVSPSE) is committed to providing the best possible care to our veterans. Information we gather from your interactions 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.

2) 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.

3) 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.aspx.

6.1b If notice was not provided, explain why.

A notice is provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

A paragraph on the homepage of the Sports4Vets community informs the Veteran of the privacy policy with the above weblink. 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, individuals have the opportunity and right to decline to provide information; however, they will likely not be able to participate in the National Rehabilitation Events if they don't enter their information.

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.

Yes, by submitting their information individuals have consented to the use of their information being used to determine if they qualify to participate in an NVSPSE event.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: Veterans are uploading their PII into the system through registering for NVSPSE events. Risk is associated with veterans not having proper notice that their PII will be retained by the tool.

Mitigation: Basic PII of veterans is utilized and all veterans consent to the use of their information by registering through the Registeration4Vets portal.

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 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 VA Public Access Link-Home (efoia-host.com) 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?

Not Applicable, 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, IAM authentication through ID.me, My HealtheVet, DS LogOn, VA Profile, Access VA. The source systems are responsible for maintaining the users data. Should an update be needed to any of the information sourced from these systems, the Veteran may contact the Event Coordinator of the event they are registering for which will facilitate notifying the system owners with needed corrections. Contact information for the Event Coordinator will be provided on the registration form.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The 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.

Registrations4Vets 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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: If Veterans provide incorrect information, they may not be selected for the program and they may not be aware how to correct their own information.

Mitigation: If the Veterans 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.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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 Program Office and Event Staff. Both have Read/Write to Registration4Vets Applications & Registration4Vets Requests and their roles identify the information and applications a user can access. The distinction between the roles is controlled by Permission Set assignments.

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?

This is not applicable. Users are from NVSPSE Office only.

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.

To receive these permissions and gain access to records with Veteran and Registration4Vets Application/Registration4Vets Request information, users must be approved by the business owner and then provisioned by the Digital Transformation Center. To receive access to the SFGCP, another 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 Registration4Vets Applications and Registration4Vets Requests, as administrators of the VA Salesforce system.

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

All development and administration is done by contractors on behalf of NVSPSE program office.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

There is no PHI.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

No, VA contractors have access to the Registration4Vets system.

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 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/31/2022
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 06/26/2023
5. *The Authorization Termination Date:* 06/26/2026
6. *The Risk Review Completion Date:* 07/07/2023
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.***
12/04/2024

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. ***(Refer to question 1.8 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 Hosting 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 3.3.1 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. CLIN SWF-5700

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.

Yes, VA has full ownership of the ancillary data stored in the system.

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.

The cloud service provider does not collect ancillary data.

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).

No robotic process automation (RPA) is used in this system.

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

ID	Privacy Controls
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: 2025.01.10 10:00:30 -05'00'

Privacy Officer, Dennis Lahl

JAMES BORING Digitally signed by JAMES BORING
Date: 2025.01.15 14:17:01 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2025.01.15 12:50:13 -05'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

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

Individuals are provided Privacy Notices for this system in multiple ways.

1) The registration site contains the following statement and link: The National Veterans Sports Programs & Special Events (NVSPSE) is committed to providing the best possible care to our veterans. Information we gather from your interactions 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.

2) 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.

3) 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.aspx.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)