



Privacy Impact Assessment for the VA IT System called:

# Salesforce - Veterans Engagement Reporting Application

## Veterans Benefits Association

### Office of Field Operations and Veteran Readiness and Employment

eMASS ID: 1935

Date PIA submitted for review:

04/12/2024

#### System Contacts:

##### *System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Renu Roy	Renu.roy@va.gov	202 263 9119
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842- 2000, Ext: 4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595- 7291

## Abstract

*The abstract provides the simplest explanation for “what does the system do?”.*

Veterans Engagement Reporting Application (VERA) solution is built on Salesforce platform for the visitors at the Regional Office (RO) to schedule appointments and receive additional information on their qualifying benefits. This solution will be used in ROs as part of the public contact team engagement with the public. This solution serves as a public contact check-in, and workflow process to serve visitors that require assistance from VA employees. These visitors can be Veterans, Dependents of Veterans, Attorney’s, and Veteran Service Organizations (VSO) that require assistance from VBA. Each request from the visitor will then go through the Salesforce VERA queue management to enable Public Contact Employee to contact the requester. VERA will display all appointments to VA Employees based on Regional Office so that VA Employees can triage these appointments and assign them to subsequent VA Public Employees to manage. The application will store the visitor’s previous request history using a phone number or email address, either collected through the portal or from the current visit. VERA will store this information on the appointment record. This data will be used to determine if the visitor had to seek assistance for the same topic on multiple occasions as well as determine which VBA Public Contact Employee previously served the Veteran/Visitor.

## 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 – Veteran Engagement Reporting Application (VERA) is controlled by Office of Field Operations and Veteran Readiness and Employment.

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

Salesforce - Veterans Engagement Reporting Application (VERA) solution is used in Regional Offices as part of the public contact team’s engagement with the public. VERA System will be used by the public and/or Veterans visiting VBA regional offices and by VA Employees in Public Contact. The system will also have a capability for offices to make an appointment online or have a VA Public Contact Employee call them back to schedule a visit to an office. VERA is a Public Contact check-in, and workflow process to serve visitors that require assistance from VA employees.

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

Salesforce Government Cloud Plus (SFGCP) is a cloud platform, data in the platform is controlled by VA but non-VA Owned and Operated. Ownership rights to PII data should be covered in the Salesforce contract. Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.

## 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?*

FY2023 had approximately 270,000 appts in VERA. The typical client is a Veteran, beneficiary, or associated representative.

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

Salesforce - Veterans Engagement Reporting Application (VERA) solution is used in Regional Offices as part of the public contact team's engagement with the public. Visitors to the Regional Office (RO) will utilize a VERA online portal to register for an appointment and receive additional information on their qualifying benefits. This request will then go through the Salesforce VERA queue management to enable Public Contact Employee to work with each request received. VERA portal allows the visitor to register and schedule an appointment through their phone or computer. Cloud Computing is being used on the Salesforce Government Cloud plus. This is a Public Contact check-in, and workflow process to serve visitors that require assistance from VA employees. VERA will display all appointments to VA Employees based on Regional Office so that VA Employees can triage these appointments and assign them to subsequent VA Public Employees to manage. VA Public Employees in Salesforce use Signal Sign On (SSO) with PIV card to access this tool. These visitors can be Veterans, Dependents of Veterans, Attorney's, and Veteran Service Organizations (VSO) that require assistance from VBA. The application will store the visitor's previous request history using a phone number or email address, either collected through the portal or from the current visit. VERA will store this information on the appointment record. This data will be used to determine if the visitor had to seek assistance for the same topic on multiple occasions as well as determine which VBA Public Contact Employee previously served the Veteran/Visitor. The system collects information on Visitor Status (Veteran, Family Member of Veteran, Attorney, Veteran Representative, Non-Veteran, and Other), Visitor Name, Phone Number, Email Address, Last four digits of SSN and Reason for the visit (Pick list of various reasons).

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

VERA application has two additional integrations to provide increased functionality,

1. Microsoft (MS) Teams integration through MuleSoft that will receive the data from Salesforce – VERA. MuleSoft will then communicate with the Microsoft Graph API to update Teams. This will aid video/ calling capability required for VERA application.
2. VA Notify Short Message Service (SMS) integration through MuleSoft to SF- VERA. This will enhance the communications between the SF-VERA application and Veterans allowing the confirmation of appointment and active tracking through text messages.

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 application is currently being used at all VBA ROs and their affiliated locations serving hundreds of thousands. VA Employees in Salesforce-VERA use Signal Sign On (SSO) with PIV card to access this tool.

### 3. Legal Authority and SORN

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

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

- Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA 36VA29/83 FR 44407 (<https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>)— Title 38, United States Code (U.S.C.), chapter 5, section 501; and chapter 3, including sections 303 and 315. Title 38 U.S.C., chapter 19; chapter 21; and section 2106. Title 5 U.S.C. 5514.
- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA. 58VA21/22/28 (<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>) – Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

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

No, the SORN does not require amendment. Yes, the two SORNs listed covers the cloud usage or storage,

- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA. [58VA21/22/28](https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf)
- Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA [36VA29/83 FR 44407](https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf)

### 4. System Changes

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

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

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

VERA is a web-based application. New integrations which include MuleSoft as a middleware which will result in technological changes.

## Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

### 1.1 What information is collected, used, disseminated, created, or maintained in the system?

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series*

(<https://vaww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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

- |   |   |   |
|---|---|---|
| <input checked="" type="checkbox"/> Name            | <input type="checkbox"/> Health Insurance       | <input type="checkbox"/> Integrated Control             |
| <input checked="" type="checkbox"/> Social Security | <input type="checkbox"/> Beneficiary Numbers    | <input type="checkbox"/> Number (ICN)                   |
| Number  | <input type="checkbox"/> Account numbers        | <input type="checkbox"/> Military                       |
| <input type="checkbox"/> Date of Birth              | <input type="checkbox"/> Certificate/License    | <input type="checkbox"/> History/Service                |
| <input type="checkbox"/> Mother's Maiden Name       | numbers <sup>1</sup>                            | <input type="checkbox"/> Connection                     |
| <input type="checkbox"/> Personal Mailing           | <input type="checkbox"/> Vehicle License Plate  | <input type="checkbox"/> Next of Kin                    |
| Address   | <input type="checkbox"/> Number                 | <input checked="" type="checkbox"/> Other Data Elements |
| <input checked="" type="checkbox"/> Personal Phone  | <input type="checkbox"/> Internet Protocol (IP) | (list below)  |
| Number(s)   | <input type="checkbox"/> Address Numbers        |   |
| <input type="checkbox"/> Personal Fax Number        | <input type="checkbox"/> Medications            |   |
| <input checked="" type="checkbox"/> Personal Email  | <input type="checkbox"/> Medical Records        |   |
| Address   | <input type="checkbox"/> Race/Ethnicity         |   |
| <input type="checkbox"/> Emergency Contact          | <input type="checkbox"/> Tax Identification     |   |
| Information (Name, Phone                            | <input type="checkbox"/> Number                 |   |
| Number, etc. of a different                         | <input type="checkbox"/> Medical Record         |   |
| individual)   | <input type="checkbox"/> Number                 |   |
| <input type="checkbox"/> Financial Information      | <input type="checkbox"/> Gender                 |   |

Other PII/PHI data elements: Visitor Status (Veteran, Family Member of Veteran, Attorney, Veteran Representative, Non-Veteran, and Other), VA email ID.

Reason for the visit (Pick list of various reasons)

### PII Mapping of Components (Servers/Database)

Salesforce – Veterans Engagement Reporting Application consists of zero 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. If there are any components, then the type of PII collected by Salesforce – Veterans Engagement Reporting Application and the reasons for the collection of the PII will be 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.**

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

*Internal Components Table*

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
N/A	N/A	N/A	N/A	N/A	N/A

**1.2 What are the sources of the information in the system?**

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

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

The information gathered by the Veterans Engagement Reporting Application (VERA) tool is collected directly from the visitor using the VERA online portal. The type of visitor can be Veterans/ Dependents of Veterans, VA Employees, VA Contractors, Volunteers, and members of the public/individual.

*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 collected directly from the visitor. This is not applicable.

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

VERA is utilized for making appointments and assisting the visitor in their request. There is no score card or analysis that is created.

**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?*

VERA is an Online portal used by the visitor. The information entered by personnel accessing the portal then goes through the Salesforce VERA queue management to enable Public Contact Employee to work with each request.

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

Information is not collected on paper; hence this is not applicable for VERA.

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

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

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

The Veteran information that is currently stored will be stored on the contact object in Salesforce. The contact object has rules to ensure no duplicate records are created.

Information is entered by the individuals who are the source.

*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?*

VERA does not utilize commercial aggregators. The information is collected online through the VERA portal is entered by the Veterans who are the source.

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

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

The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. Additionally, the two SORNs applicable for the system provides the authority for collection of information as follows,

- Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA 36VA29/83 FR 44407 (<https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>) – Title 38, United States Code (U.S.C.), chapter 5, section 501; and chapter 3, including sections 303 and 315. Title 38 U.S.C., chapter 19; chapter 21; and section 2106. Title 5 U.S.C. 5514.
- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA. 58VA21/22/28 (<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>) - Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

#### **1.6 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:** A visitors' basic information such as the name, contact number, address can be at a risk of exposure. Depending on the reason of the visitor, particular veteran visiting the facility can be identified.

**Mitigation:** Only a VA Employee with PIV SSO to VERA portal will be able to contact the visitor or view the PII of any individual using the portal to set up an appointment. Data is encrypted by Salesforce Shield Platform which provides FIPS 140-2 certified encryption. Additionally, all data and content stored in Salesforce Government Cloud Plus (SFGCP) is encrypted.

## 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
Visitor Status (Veteran, Family Member of Veteran, Attorney, Veteran Representative, Non-Veteran, and Other)	Used as an Identifier	Not used
Visitor Name	Used as an Identifier	Not used



Phone Number	Used to contact individual and confirm the visitation request	Not used
Email Address	Used to contact individual and confirm the visitation request	Not used
Reason for the visit (Pick list of various reasons)	Used by Regional Office to assist the visitor	Not used
Last four of SSN	Used to identify the Veteran and assist in their visitation request	Not used
VA Email ID	Used to identify the VA employee assisting the Veteran. It is also used as login to the VERA application	Not Used

**2.2 What types of tools are used to analyze data and what type of data may be produced?**

*These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.*

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

Salesforce Government Cloud Plus (SFGCP) is used to track the data in the system. Based on the data entered by the visitor, a VA Employee would be able to assist. A VA employee can contact the visitor to schedule an appointment and/or answer any questions on their benefits. The information of the VA employee assisting each of the visitor is retained in the system. The number of attempts by the visitor for the reason of visit is also captured. No analysis is performed on the information collected through the requesting portal.

*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.*

When a new record is created. Newly created information is accessible to VA employees for appointment purposes only, no determinations are made from these appointments.

**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?*

VERA is accessed via a secured webpage utilizing Single Sign On (SSO) technology. VERA is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls

in place for safeguarding the data stored there. The data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Product provides FIPS 140-2 certified encryption. Encrypted interconnection between VERA and two other systems Microsoft Teams – MS Graph API and VA Notify API allows data flow through a secure certificate MuleSoft API.

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

Fields such as SSN are protected by Salesforce Shield Protect which provides FIPS 140-2 certified encryption. The SORN (Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA [36VA29/83 FR 44407](#) and Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA [58VA21/22/28](#)) defines the information collected from veterans, use of the information, and how the information is accessed and stored. VERA tool retains the information of the VA employee who assisted the visitor, if the request is a new one, and /or if the request is repeated enquiry for the same reason.

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

VERA is accessed via a secured webpage utilizing SSO technology. VERA tool is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

## **2.4 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?*

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

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

Access to the VERA system is requested by the employee's supervisor and approved by the system owner through DTC. All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):

- 1) Logon / Logoff
- 2) Create Data
- 3) Update Data
- 4) Delete Data

*2.4c Does access require manager approval?*

Yes, supervisor/manager approval is required for new users accessing VERA application.

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

Profile-based setting available in Salesforce is leveraged for users access in VERA application. User have limited access to PII information captured in the tool and access is monitored using logging details available through Salesforce cloud technology.

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

VERA is accessed via a secured webpage utilizing SSO technology. VERA is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is applied based on FedRAMP Salesforce Gov Cloud Plus 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 VERA 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*

The information retained for assisting the visitor are:

- Visitor Status (Veteran, Family Member of Veteran, Attorney, Veteran Representative, Non-Veteran, and Other)
- Visitor Name
- Visitor Phone Number
- Visitor Email Address
- Reason for the visit (chosen amongst a list of various reasons).
- VA Employee Name
- VA Email ID
- Last 4 of SSN

### 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.*

Records management within the Department of Veterans Affairs is governed by VA Directive 6300, Records and Information Management with specific records management procedures documented in VA Handbook 6300.1. 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 applicable to the system can be found at the following link: <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf> is as follows,

- Item # 7900, Title – The Caregiver Record Management Application (CARMA), Disposition - Temporary; Destroy 75 year(s) after enrollment under the authority DAA-0015-2020-0001-0001.
- Item # 1180.17, Title – Veterans Benefits, Disposition - PERMANENT. Cutoff after receipt of last relevant correspondence. Transfer to NARA 50 years after cutoff.

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

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

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

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

VERA complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the VERA instance will be retained as long as the information is needed in accordance with VA Records Control Schedule VB-1, Part 1. Specific retention periods can be located in the VB-1 document at the following URL:

<https://www.benefits.va.gov/WARMS/21guides.asp>

Additionally, the retention schedule for Salesforce Government Cloud Plus (SFGCP) also applies to Salesforce – VERA.

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

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

1. Item # 7900, Title – The Caregiver Record Management Application (CARMA), Disposition - Temporary; Destroy 75 year(s) after enrollment under the authority DAA-0015-2020-0001-0001.
2. Item # 1180.17, Title – Veterans Benefits, Disposition - PERMANENT. Cutoff after receipt of last relevant correspondence. Transfer to NARA 50 years after cutoff under disposition authority N1-15-06-2, item 18.
3. Item # 07-706.000, Title - Supporting documentation maintained in VR&E Central Office on Administrative Reviews, Disposition - Maintain in inactive files in VR&E Central Office and destroy by shredding 3 years after date of last activity.

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to the Record Control Schedule 10-1 Section 4 (Disposition of Records).

### **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.*

The Salesforce – Veterans Engagement Reporting application adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)

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

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what*

*controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.*

VERA does not use PII for research, testing and training. Basic Privacy Training is required to be completed by the VA employee before they are authenticated to use the VERA tool. VA Handbook 6500 mandates that systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.

### **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:** The risk to maintaining data within VERA is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

**Mitigation:** To mitigate the risk posed by information retention, the VERA Module adheres to the VA RCS 10-1 and SORN retentions. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*

*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

### Data Shared with Internal Organizations

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Microsoft Teams – MS Graph API		Visitor name, date and time of appointment, reason for the visit	Encrypted interconnection via a security certificate through MuleSoft API
VA Notify API		Visitor name, date and time of appointment, reason for the visit	Encrypted interconnection via a security certificate through MuleSoft API



<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>

#### **4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

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

Follow the format below:

**Privacy Risk:** The basic information of the visitor such as the name, contact number and email address and reason for visit will be at the risk of exposure.

**Mitigation:** The VA requires single sign-on (SSO) or two-factor authentication (2FA) in order to access VERA. The following security control families are applicable (in addition to all NIST applicable RMF families):

- Audit and Accountability
- Awareness Training
- Security Assessment and Authorization
- Incident Response Personnel Security
- Identification and Authentication

The tool will have a definable “time-out” setting which will automatically log the user out after a period of inactivity.

## **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**

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
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:** VERA retains visitor PII information.

**Mitigation:** No data is shared externally.

## Section 6. Notice

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

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

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

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

Notice to Visitors is provided in three ways,

1. VERA online portal, the visitor is requested to fill in the basic information, this provides as a notice for the personnel that the information can and will be used to contact them.
2. Specifically, any information that relates to collection from an individual is collected and maintained in an alternate system which is covered under SORN Access to the PII is described by the System of Records Notice (SORN) for the SF-VERA application can be found online at [https://www.oprm.va.gov/privacy/systems\\_of\\_records.aspx](https://www.oprm.va.gov/privacy/systems_of_records.aspx).
3. This Privacy Impact Assessment (PIA) also serves as a notice of VERA application.

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

Notice is provided through a disclaimer on VERA online portal, SORN and this PIA.

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

Notice is provided through a disclaimer on VERA online portal, SORN and this PIA.

**6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?**

*This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.*

No, the individual cannot decline if they need the service of the VA employee to reach out to them in case of assistance with scheduling.

**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, the individual is consenting to the right to have a VA Employee contact them in case for scheduling an appointment at the VBA RO office.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

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

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** The information gathered by the visitor can be at risk of exposure if they were not aware about it at the time of providing the information.

**Mitigation:** The VA mitigates this risk by providing the public with three forms of notice, as discussed in detail in question 6.1, including disclaimer on VERA online portal, this Privacy Impact Assessment and the associated System of Record Notice (SORN).

## Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

### 7.1 What are the procedures that allow individuals to gain access to their information?

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

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at <http://www.foia.va.gov/> to obtain information about FOIA points of contact and information about agency FOIA processes.*

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

Individuals would need to submit a FOIA or Privacy Act request in order to obtain copies of the information stored in VERA. Per the SORNs, the following are the procedures for accessing the records:

- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA (58VA21/22/28) - submit requests to the FOIA/ Privacy Act Officer at the VA Regional Office serving the individual's jurisdiction. Address locations for the nearest VA Regional Office are listed at VA Locations Link. [Find VA Locations | Veterans Affairs](#)
- Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA (36VA29) - Individuals desiring access to, or wishing to contest, VA records and related procedures should write to the VA Insurance Center at 5000 Wissahickon Avenue, Director's Office (29), Philadelphia, Pennsylvania 19144.

*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)?*

VERA is not exempt from Privacy Act.

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

Veterans can gain access to their information through FOIA as shown in section 7.1a.

### 7.2 What are the procedures for correcting inaccurate or erroneous information?

*Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1,*

state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

While inaccurate information should not likely appear due to contact object rules already established, there is a potential for inaccurate information in any source systems. Inaccurate information can be reconciled manually by end users or by creating a ticket to Digital Transformation Center (DTC) requesting to reconcile data. DTC is the contract team responsible for the administration and management of the Salesforce platform.

### **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.*

Employees may be notified by either the Veteran or Visitor to correct existing information or by another internal VA employee. The process by which corrections can be made are outlined in 7.2.

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

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

*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

This is not applicable for VERA. Veterans will have to request their information through FOIA requests.

### **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:** There is a risk that information of visitors may be incorrect, and those visitors are unaware of how they can access or correct their information in the system.

**Mitigation:** By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files. Furthermore, this document and the SORN provide the point of contact (POC) for members of the public who have questions or concerns about applications and evidence files. All access and redress issues are utilizing the same POC. Prior written consent or a power of attorney authorizing access is required before VA will allow the representative or attorney to have access to the claimant's automated claims records. Contact information is listed by facility in the SORN.

Additionally, Individuals can submit a FOIA or Privacy Act Request to obtain a copy of their information in the system. However, because the data in VERA is from the Contact object, which is provided by the MPI, the PIA for MPI should provide additional mitigation strategies.

## **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?*

Yes, new users access the system with supervisor/managerial approval. User roles identify the information and applications a user can access. To receive access to the system, another user 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 control of the information and data.

#### *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?*

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



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

Following are the roles and access for VERA.

Role	Responsibilities and Access Type
VA Employee Access	Manage appointments
Local Administrator	Manage appointments, manage resources, manage service Territories under their jurisdiction, manage work types
National Administrator	Manage appointments, manage resources, manage service territories, manage work types, create new territories
Quality Reporting	Read only access to data

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

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

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

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

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

General Training includes: VA Privacy Rules of Behavior, Privacy awareness training, HIPAA and VA on-boarding enterprise-wide training. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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

*8.4a If Yes, provide:*

- 1. The Security Plan Status: Approved*
- 2. The System Security Plan Status Date: Not yet approved.*
- 3. The Authorization Status: Active*
- 4. The Authorization Date: 06/01/2023*
- 5. The Authorization Termination Date: 06/01/2024*
- 6. The Risk Review Completion Date: 06/01/2023*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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

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

*This is not applicable.*

## **Section 9 – Technology Usage**

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

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

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

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

Yes, the Salesforce – Veterans Engagement Reporting Application (VERA) utilizes Salesforce Government Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. MuleSoft middleware integration allows dataflow through different systems.

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

Yes, VA has full ownership of the PII/PHI that will be shared through the Salesforce – Veterans Engagement Reporting Application (VERA). Contract agreement “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B.

**9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?**

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

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

**9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

VA has full authority over data stored in VERA.

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

*Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the*

*automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).*

Salesforce – Veterans Engagement Reporting Application (VERA) does not utilize RPA.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
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.**

---

**Privacy Officer, Renu Roy**

---

**Information System Security Officer, James Boring**

---

**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).

Two SORNs applicable for the system:

- Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA 36VA29/83 FR 44407 (<https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>)
- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA. 58VA21/22/28 ( <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>)

VB–1, Part 1 document is located at, <https://www.benefits.va.gov/WARMS/21guides.asp>.



## **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](#)