Privacy Impact Assessment for the VA IT System called:

Salesforce – VRE Business Accounts Management System (SF-VREBAMS)

Veterans Benefits Administration

Veteran Readiness & Employment Service (VR&E)

eMASS ID: TBD

Date PIA submitted for review:

02/10/2025

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)	*Joseph Facciolli*	*joseph.facciolli@va.gov*	*215-842-2000 x2012*
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 – VRE Business Accounts Management System (SF-VREBAMS) is a Customer Relationship Management (CRM) tool designed to provide an overview on a national, regional, state, and local level of Business Accounts and the Employment Coordinators (EC) activities in managing the lifecycle of a Veteran employment placement. The VR&EBAMS would provide an efficient manner to track employment related activities to include development of business partnerships, maintenance of current business partners, job leads and referrals, outreach activities and events, labor market data, and quick, reliable statistics related to all data maintained. The Employment Coordinator (EC) role is to assist veteran participants with obtaining employment by leveraging opportunities through known businesses. Businesses are managed from either a national, regional, or state level. The system would also track special hiring program such as Non-Paid Work Experience (NPWE), Special Employer Incentive (SEI), and On The Job Training (OJT).

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?*

   SF-VREBAMS is a Customer Relationship Management (CRM) tool designed to provide an overview on a national, regional, state, and local level of Business Accounts and the Employment Coordinators (EC) activities in managing the lifecycle of a Veteran employment placement.

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.*

   SF-VREBAMS is a VA-owned Salesforce-controlled system built on the Salesforce Government Cloud Plus – Enterprise (SFGCP-E).

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?*

   This system serves as a repository for Veterans nationwide and business partners. This could exceed 100,000+ individuals.

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?*

The SF-VREBAMS would provide an efficient manner to track employment related activities to include development of business partnerships, maintenance of current business partners, job leads and referrals, outreach activities and events, labor market data, and quick, reliable statistics related to all data maintained.

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

SF-VREBAMS is a stand-alone system. It does not have internal and external connections to share information.

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

Yes

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, the system does not operate in more than one site. SF-VREBAMS is built on the underlying Salesforce.com and Salesforce Government Cloud Plus – Enterprise (SFGCP-E) is hosted on AWS Government Cloud.

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?*

The SORN provide the legal authority to operate.
58VA21/22/28 / 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA 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.

H. What is the SORN?

58VA21/22/28 / 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

I. SORN revisions/modification

Currently, there is no revision/modification needed.

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

Currently there is no modification, amendment or revision and approval needed.

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
□ Sex
□ Integrated Control Number (ICN)
□ Military History/Service Connection
□ Next of Kin
□ Date of Death
□ Business Email Address
□ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: Job Lead Veteran Referred (specific job lead number the Veteran was referred to, Job Title, Station Associate with referral (3-digit number that identifies the station associated with the Veteran), VA Phone Number, VA Email Address, Business Name, Business Point of Contact (POC) Name, Business Point of Contact (POC) Phone Number, Business Point of Contact (POC) Email Address, Business City, Business State, Business Zip, Business Sector Type, Business Partnership, Business Education Coordinator Name, Business Station

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

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 VA Employment Coordinators (EC) who is assisting the Veteran participants will be collecting the information from the Veterans.

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 from the veteran.

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

Yes, the system will create reports of the overview lifecycle of the veteran employment placement.

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 VA Employment Coordinators (EC) will be collecting the information from the Veterans.

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?

The information is not collected on a form.

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.

No, information stored in the system does not check against any other source of information for accuracy.

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

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

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

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 SORNs applicable for the system provides the authority for collection of information as follows.

58VA21/22/28 / 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA 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: *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: The Veteran data and members of public data captured in this tool poses a risk of exposure.

Mitigation: The data secured in Salesforce Shield which utilizes FIPS 140-2 encrypted connection. Only authorized internal VA users login via single sign on to the application.

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	Used as an Identifier to the individual	Internal
Last Name	Used as an Identifier to the individual	Internal
File Number (Last 4 digits of SSN)	Used as an Identifier to the individual	Internal
Job Lead Veteran Referred (specific job lead number the Veteran was referred to)	Used to reference job opening positions	Internal
Job Title	Used to reference job opening positions	Internal
Station Associate with referral (3-digit number that identifies the station associated with the Veteran)	Used as an identifier for VR&E Office location.	Internal
VA Phone Number	Used as an Identifier to the individual	Internal
VA Email Address	Used as an Identifier to the individual	Internal

Business Name	Used to identify the business partner	Internal
Business Point of Contact (POC) Name	Used as an Identifier to the individual	Internal
Business Point of Contact (POC) Phone Number	Used as an Identifier to the individual	Internal
Business Point of Contact (POC) Email Address	Used as an Identifier to the individual	Internal
Business City	Used to identify the business partner	Internal
Business State	Used to identify the business partner	Internal
Business Zip	Used to identify the business partner	Internal
Business Sector Type	Used to identify the business partner	Internal
Business Partnership	Used to identify the business partner	Internal
Business Education Coordinator Name	Used as an Identifier to the business individual	Internal
Business Station	Used as an Identifier for business partner department and location.	Internal

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?

The system will generate reports to provide lifecycle of Veterans employment placement opportunities and the vacancies available by partner organizations. The information derived will be veteran name, organization name, and dates.

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.

Information collected on an individual will not create new records.

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 application utilizes Salesforce Shield protect adhering to FIPS 140-2 encrypted connection protests 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).

Yes, the last 4 digits of the Social Security Number is capture. Salesforce Shield Protect, which provides FIPS 140-2 certified encryption. All data stored in Salesforce Government Cloud Plus – Enterprise (SFGCP-E) is encrypted.

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

Users accessing VRE-BAM must be authenticated during login and granted access based on role. Additionally, PII in Salesforce applications is encrypted and each user that has access to the Salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>*Principle of Transparency:*</u> *Is the PIA and SORN, if applicable, clear about the uses of the information?*

<u>*Principle of Use Limitation:*</u> *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 in stored in the system is based on role hierarchy.

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?

1. VA and Salesforce have implemented required security and privacy controls for Federal Information Security Modernization Act (FISMA) according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

2. New users submit a request for access through the Digital Transformation Center (DTC). The DTC then assigns the request to the individuals who have administration access to the module and the access is then granted or denied based on the information the user provided by the administration. The DTC is then notified of the approval/disapproval and DTC takes action on the request based on the administration's response. Requests, approvals, and denials of access are recorded within Salesforce.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, all electronic records with PII are stored within Salesforce for authorized users. All workflows are completely electronic.

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

Privacy Officer, Information System Security Officer and Information Security Officer are responsible for all safeguards to be put into place to protect the PII. Noting that Salesforce encryption is established.

Section 3. Retention of Information

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

3.1 What information is retained?

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

- First Name
- Last Name
- File Number (Last 4 digits of SSN)
- Job Lead Veteran Referred (specific job lead number the Veteran was referred to
- Job Title

- Station Associate with referral (3-digit number that identifies the station associated with the Veteran)
- VA Phone Number
- VA Email Address
- Business Name
- Business Point of Contact (POC) Name
- Business Point of Contact (POC) Phone Number
- Business Point of Contact (POC) Email Address
- Business City
- Business State
- Business Zip
- Business Sector Type
- Business Partnership
- Business Education Coordinator Name
- Business Station

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 could be retained for 5+. Active cases could ongoing and archived could be purged after 5 years.

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. 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).

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

Decisions to destroy VR&E paper counseling records are to be made in accordance with Records Control Schedule (RCS), RCS VB–1, Part I, Field in Section VII, dated January 31, 2014. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education file folders in paper are retained at the servicing Regional Processing Office. Education paper folders may be destroyed in accordance with the times set forth in the VBA Records Management Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.

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.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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.

SF-VRMBAMS does not use veteran PII information 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:

<u>Principle of Minimization:</u> 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.

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> If retention time is exceeded the risk to exposure of PII is increased by unauthorized individuals.

<u>Mitigation:</u> All data at rest in Salesforce platform is encrypted with Salesforce Shield which utilizes FIPS 140-2, in addition to being protected by FedRAMP security controls under the FedRAMP AT 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 SF-VREBAMS consists of **2** 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 SF-VREBAMS 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)	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

etc.) that contains PII/PHI					
Salesforce Government Cloud Plus – Enterprise (SFGCP-E)	Yes	Yes	First Name, Last Name, File Number (Last 4 digits of SSN), Job Lead Veteran Referred (specific job lead number the Veteran was referred to, Job Title, station Associate with referral (3-digit number that identifies the station associated with the Veteran), VA Phone Number, VA Email Address, Business Name, Business Point of Contact (POC) Name, Business Point of Contact (POC) Phone, Number, Business Point of Contact (POC) Email Address, Business City, Business State, Business Zip, Business Sector Type, Business Partnership, Business Education Coordinator	Salesforce Government Cloud Plus – Enterprise (SFGCP-E) is a cloud platform, in which VRE Business Accounts Management System (SF-VREBAMS) was built on and leverages the database to collect and store information. The PII is used by the Salesforce-The Bridge for reporting purposes.	VRE Business Accounts Management System (SF-VREBAMS) is an minor system hosted on the cloud SFGCP platform, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there.

			Name, Business Station		

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***
N/A	N/A	N/A	N/A

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

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:

<u>Privacy Risk:</u> The PII will be at the risk of exposure.

<u>Mitigation:</u> The VA requires SSO or two-factor authentication (2FA) in order to access 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 be more than one)*	*List the method of transmission and the measures in place to secure data*

N/A	N/A	N/A	N/A	N/A

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

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> There is no external sharing.

<u>Mitigation:</u> 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.

A notice is provided when the Veteran completes and checks the appropriate box on the Application for Veteran Readiness & Employment Benefits for Claimants with Service Connected Disabilities (28-1900). VA Form 28-1900

Notice includes the following statement:
My giving the requested information is voluntary. I understand that the following results might occur if I do not give this information:

(1) *I may not receive the maximum benefit either from counseling or from my education or rehabilitation program.*
(2) *If certain information is required before I may enter a VA program, my failure to give the information my result in my not receiving the education or rehabilitation benefit for which I have applied.*
(3) *If I am in a program in which information on my progress is required, my failure to give this information may result in my not receiving further benefits or services. My failure to give this information will not have a negative effect on any other benefit to which I may be entitled."*

A copy is link to Appendix A.

6.1b If notice was not provided, explain why.

A notice is provided. See above 6.1a.

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

The notice is provided on the Application for Veteran Readiness & Employment Benefits for Claimants with Service Connected Disabilities (28-1900).

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

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

Yes, if the Veteran declines to provide information, VR&E benefits will not be provided. However, this doesn't affect any of their other VA benefits. This is stated on the 28-1900.

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 related to VR&E Services.

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: Review of the PIA document on Salesforce – VRE Business Accounts Management System (SF-VREBAMS) for Veterans Benefits Administration office of Veteran Readiness & Employment Service (VR&E) poses no identifiable Privacy Risk associated with *potentially insufficient notice*. Please review section 6.1a and 6.1c for additional details on this Privacy risk .

Mitigation: No Mitigation required.

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.***

RECORD ACCESS PROCEDURES:
Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type

of information or records an individual is seeking will determine the location to which a request should be submitted. Authorized requestors should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690.

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)?

SF-VREBAMS is not exempt from Privacy Act.

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

The procedure is the same as 7.1a.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The Employment Coordinator will have permissions to change or modify information within the system.

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 type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, DID: 608–373–6690.

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.

Formal redress is provided for this system as noted in answer 7.3 above.

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: The individual may not know how to redress, access or provide correction to data.

Mitigation: The information to correct or amend information is included in this PIA which is available for public record. Veterans have the right to amend by putting their request in writing.

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?

As a part of the onboarding process, the individual and or Supervisor/Veteran Readiness& Employment Service Officer (VREO) will submit a request utilizing the DTC User Provisioning application. DTC Helpdesk submits the request to the named supervisor/VREO for review and approval. DTC grants appropriate access (ensuring the users are granted only the named privileges needed to access and perform duties to VRE BAMS.

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?

Only VA Employees have access to the application.

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.

Roles	**Access Type**
Employment Coordinator	Read, Write, Edit, View, Modify
National Employment Coordinators	Create, Read, Edit, Delete, View, Modify
Veteran Readiness & Employment Manager (VREO)	Read, Edit, Delete, View, Modify
Central Office Admin	Read, View

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

No, VA Contractors will not have access to this application.

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

Contractors will be involved in the design, development, and maintenance of the system. Contractors have signed Non-Disclosure Agreements (NDA).

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 captured in the tool, so this is not applicable.

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.

Yes, there is a NDA in place.

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, HIPPA and VA on-boarding enterprise-wide training. Users 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 as part of the security awareness training that all personnel must complete via VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:*
2. *The System Security Plan Status Date:*
3. *The Authorization Status:*
4. *The Authorization Date:*
5. *The Authorization Termination Date:*
6. *The Risk Review Completion Date:*
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.***
05/15/2025

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, the SF-VREBAMS utilizes Salesforce Government Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus Enterprise (SFGCP-E) 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. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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 Salesforce – Veterans Engagement Reporting Application (VERA). Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B23F0172.

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

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

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

No, CSP will not collect any ancillary data in this 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.

Yes. The VA is utilizing Salesforce Gov Cloud Plus. Information is only shared internally.

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

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

SF-VREBAMS does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

RENU ROY

Digitally signed by RENU ROY
Date: 2025.03.25 10:42:59
-04'00'

Privacy Officer, Renu Roy

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2025.03.25 14:02:53
-04'00'

Information System Security Officer, Joseph Facciolli

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2025.03.25 14:52:43 -04'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

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

VA Form 28-1900

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)