Privacy Impact Assessment for the VA IT System called:

Veterans Enterprise Management System (VEMS)

Office of Small & Disadvantaged Business Utilization (OSDBU)

Veterans Affairs Central office (VACO)

Date PIA submitted for review:

03/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tyrone Brown	Tyrone.Brown@va.gov	202-632-8204
Information System Security Officer (ISSO)	Bernadette Bowen-Welch	Bernadette.BowenWelch1@va.gov	202-340-8970
Information System Owner	Carol Cleveland	Carol. Cleveland@va.gov	202-461-4291

Abstract

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

Veterans Enterprise Management Systems (VEMS) is an enterprise solution platform that provides access to all applications resident in the VetBiz Portal, Event Management Software as a Service (EMSS), VetBiz Stat, Enhanced Vendor Profile (EVP), Electronic Request for Information (eRFI), Forecast of Contracting Opportunities (FCO) and other static information). VEMS has significantly enhanced OSDBU's ability to accomplish its VA mission to expand small business participation in federal procurement opportunities.

The system also provides Government-wide access to promote sharing of data and resources between the different Government agencies that have common desired outcomes. VEMS has increased VA staff access to Goals Management, Risk Management, Acquisition Analytics, and Market Research tools.

VEMS uses state-of-the-art IT solutions to increase automation and improve efficiencies by integrating standalone systems to provide centralized access to Goals Management, Risk Management, Acquisition Analytics, Market Research tools and Event Registration and Management. VEMS utilizes Microsoft Dynamics 365 SaaS Customer Relationship Management (CRM) platform and PowerApps Portals platform on the Microsoft Azure Government Cloud to support all OSDBU Business Processes.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

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

Veterans Enterprise Management System (VEMS) Veterans Affairs Central Office (VACO)

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

The Office of Small and Disadvantaged Business Utilization (OSDBU) developed VEMS to provide an Information Technology (IT) infrastructure that would enhance OSDBU's ability to accomplish its VA mission to expand Small Business (SB) participation in Federal procurement opportunities. The VetBiz Portal is a PowerApps Single Sign-On (SSO) interface with Dynamics 365 CRM. Mission/Business processes, such as the Call Center, provide Veterans and Small Business Owners with acquisition assistance. VetBiz Stat provides information lookup concerning Goals Management, Risk Management, Acquisition Analytics, and Market Research tools. Vendor Event Matchmaking System allows single sign-on access to all OSDBU events and training.

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

OSDBU

2. Information Collection and Sharing

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

183,048+

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

The Office of Small and Disadvantaged Business Utilization (OSDBU) has modernized its Information Technology (IT) environment to significantly enhance its ability to accomplish its mission to expand Small Business (SB) participation in Federal procurement opportunities and promote Veterans First Contracting Program. Through this effort, OSDBU has implemented an Enterprise level Information System based upon a Service Oriented Architecture (SOA) to integrate existing and future systems. The Veterans Enterprise Management System (VEMS) is a software as a service (SaaS) application that provides Veterans and other stakeholders with a unified user-experience via a single-window interface for all enterprise functionalities, applications, and services. The VEMS system will support a best-in-class risk analysis, business intelligence, market research, acquisition support, goals management, predictive analytics, direct access, outreach, event management and training experience for internal and external stakeholders. The VetBiz Portal is the gateway into the VEMS system. The SaaS VetBiz Portal leverages PowerApps and connects with Vendor Event Matchmaking System (VEMMS). External users use AccessVA for signing on and then access VA posts the assertions to Azure B2C tenant which in turns send the assertions to the VetBiz Portal. Both VetBiz Stat (Fedmine) and Vendor Event Matchmaking System (VEMMS) are external IT systems where data is shared/transmitted with VEMS.

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

Call Center Services – Helpdesk to Veterans calling for acquisition assistance. VetBiz Stat (Fedmine) External Connection - there is no VA owned data transmitted to SMARTPROCURE FEDMINE LLC US via the interconnection. VEMS queries Fedmine and information is returned via database pull to VEMS. Vendor Event Matchmaking System (VEMMS) (My Business Matches) – External Connection – Vendor Owner profile data is collected via encrypted API from VEMS and placed on a form within VEMMS to assist VetBiz users with event registration.

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

Not Applicable

3. Legal Authority and SORN

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

- The VEMS system has been approved as the System of Records to execute the aforementioned charge as detailed in VA SORN 181VAOSDBU.

- The VEMS application complies with the following federal regulations and/or departmental policies and guidelines, as follows:
  - Title 38, United States Code, Section 501-Veterans' Benefits.
  - Title 38 United States Code, Section 8127 -Small Business concerns owned and controlled by veterans, contracting goals and preferences.
  - Small Business Act, Section 15(k)
  - VHA Directive 2009-021 Data Entry Requirements for Administrative Data
  - OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
  - Public Law 108–183 (December 2003), the Veterans Benefits Act of 2003, Sections 301, 305, 308.
  - Public Law 106–554 (December 2000), Sections 803 and 808.
  - Public Law 106–50 (August 1999), the Veterans Entrepreneurship and Small Business Development Act of 1999.
  - Public Law 105–135 (December 1997), Title VII, Service-Disabled Veterans Program.
  - Public Law 93–237 (January 1974), Special Consideration for Veterans.
  - Public Law 106–50, Section 302, Entrepreneurial Assistance, subsection (5).
  - VA Directive 6300, Records and Information Management
  - VA Handbook 6500, VA6500 AC-8: System Use Notification
  - The Privacy Act of 1974

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

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
No

K. *Whether the completion of this PIA could potentially result in technology changes*
NO

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

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

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

- Contract Acquisition Data Revenue
- EnvironmentIdentifier
- agencyContract,
- figures
- Position title
- VISN, Office,
- Provider Id.
- FedmineModule,
- UserID
- (Guid),
- CompanyCertification
- CompanyOrg

- extentContract,
- GSAContract
- SAM UEI.
- IsVerified
- Primary Email,
- Company Type
- BondingLevel,
- CveVerificationDate,
- YearEstablished,
- EmployeesNumber,
- EmployeesNumberVet,
- IsVeteran
- IsMinorityOwned,
- IsServiceDisabled,
- IsWOSB,
- CertifiedCor
- Contract acquisition data revenue
- Sec Id
- (Guid),
- Title of an event,
- Date of an event,
- Location,
- CompanyName,

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

PII Mapping of Components (Servers/Database)

VEMS consists of one key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VEMS and VetBiz Portal 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

Veterans Enterprise Management System (VEMS)-VetBiz/CRM. Database (dvagov-vems)	**No**	**NO**	Name, Mailing Address, Zip Code, Phone Number(s)- personal and/or business, Fax Number, Company Name, Email Address – personal and/or business, Security ID (SecID), Last Name, First Name, Middle Name, Prefix, Suffix, Address line 1, City, State, Country, Postal Code, Principal Name (UPN), Provider Id	To support OSDBU small business programs in accordance with (IAW) Small Business Act (15K). Public company information is collected for market research for contracting opportunities.	To access data user must have token granted by Access VA credentialing Service Provider. ID.me, DS Logon, or VA PIV. Non-VA users will not have direct access to the CRM Database. Non-VA users utilizing the ID.me or DS Logon credential provider will only be granted access to view their personal profile data via VetBiz Portal, the system's web app graphical user interface (GUI) VA acquisition officials will not have direct access to the CRM DB but can request access to the enhanced Vendor Profile application. This will grant approved acquisition officials' access to vendor PII for the purposes of Market Research via web-based application. This access will require authentication via an VA issued PIV. Only system administrators with NMEA zero tokens approved by the system owner and the VA infrastructure operations group can access. In addition, the sys admin also requires provisional approval from VAEC to

					access any hosted SaaS infrastructure.

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?

Data is supplied by the veteran but is confirmed via integrated external systems and data sources, these systems will either be connected through web services or provide scheduled updates to the back end VEMS database. The following tables include a list of internal-to VA and external systems and data sources which are currently used by the system.

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

Information is coming from external IT systems such as VetBiz Stat (Fedmine) and Vendor Event Matchmaking System (VEMMS) (My Business matches). Vendor Owner profile data collected via encrypted API from VEMS and placed on a form within VEMMS to assist VetBiz users with event registration. The interconnection between VEMS and VEMMS is a two-way path. Public vendor data is acquired via the API from VEMS to ensure the integrity of data within VEMMS profile. Fedmine is a SaaS solution that provides users within the federal acquisition community real-time visibility into federal spending and other related business activities. Leverages the internet to aggregate federal data from disparate sources and then maximizes its relevancy for many government users.

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

Procurement Decision makers and Acquisition professional use CRM to produce reports & dashboards specific to vendor under consideration in market research and acquisition analysis.

1.3 How is the information collected?

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

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

The information is collected directly from the individual and other internal/external data sources via an electronic form. Internal/external data sources include end users, the Veterans Enterprise Management System and the internal Credential Service Provider. Customers may also contact a system administrator via email, or telephone for assistance. These interactions will be logged and associated with the user's profile. The user may contact an OSDBU Program area directly but will primarily engage a Customer Service Representative (CSR) within the OSDBU Call Center for Tier 1 assistance

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

Information is not collected on a form.

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

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

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

> Data validation applies to individual data fields
>
> Information in user profiles will be validated by the information provided by the credentialing service provider when the user logs into the VetBiz Portal. Centralized Data Validation: The integration layer will implement a standard set of validation rules based on the data definitions defined by the data model. This ensures that a common set of rules are applied across applications. Applications may implement more restrictive rules but cannot override the rules defined in the integration layer.

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

VEMS leverages Access VA and utilizes all three credentialing service providers. The accuracy of the data depends on the accuracy of the credentialing service contracted with Access VA.

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 VEMS system has been approved as the System of Records to execute the aforementioned charge as detailed in VA SORN 181VAOSDBU.

The VEMS application complies with the following federal regulations and/or departmental policies and guidelines, as follows:

- Title 38, United States Code, Section 501-Veterans' Benefits.
- Title 38 United States Code, Section 8127 -Small Business concerns owned and controlled by veterans, contracting goals and preferences.
- Small Business Act, Section 15(k)
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- Public Law 108–183 (December 2003), the Veterans Benefits Act of 2003, Sections 301, 305, 308.
- Public Law 106–554 (December 2000), Sections 803 and 808.
- Public Law 106–50 (August 1999), the Veterans Entrepreneurship and Small Business Development Act of 1999.
- Public Law 105–135 (December 1997), Title VII, Service-Disabled Veterans Program.
- Public Law 93–237 (January 1974), Special Consideration for Veterans.
- Public Law 106–50, Section 302, Entrepreneurial Assistance, subsection (5).
- VA Directive 6300, Records and Information Management
- VA Handbook 6500, VA6500 AC-8: System Use Notification
- The Privacy Act of 1974

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:

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

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: Not Applicable. VEMS no longer collect documents from Veterans. This will be highlighted in the SORN as we are not keeping the documents or collecting new documents

Mitigation:
1, Veteran information is validated through VA's Enterprise Identity and Access Management (IAM), as the authoritative source, before a call proceeds and any information is provided. Additional information gathered and provided is based on IAM-returned identifiers. The CSR will be aware of incorrectly entered data because the IAM search will return zero records or the IAM results will return a Veteran, sponsor (Veteran) who is not the subject of the call. The CSR must validate that the correct Veteran is returned from the search before the CSR can proceed to review eligibility information. If the Veteran is not validated the CSR ends the call.
2, Veteran information is validated through internal VA systems, including the Veterans Enterprise Management System, VA's Enterprise Identity and Access Management (IAM) services and other authoritative data sources. The Customer Service Representative (CSR) or OSDBU staff members do not provide PII as a means of selecting the correct user profile.
3, The VetBiz Portal web interface to VEMS ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the VetBiz Portal is through AccessVA, which provides a single-entry point for access to many VA websites and online applications. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. All VA staff members with higher level access to the VetBiz Portal are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) training annually.

Section 2. Uses of the Information

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

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

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

Information is submitted on web forms in VEMS. OSDBU uses the basic user information and company information in support of OSDBU's mission including Strategic Outreach, Communications and Training Programs and Acquisition Support Programs.

Data Attribute	Description
• First Name	First Name of Veteran or User
• Middle Name	Middle Name of Veteran or User
• Suffix	Suffix of Veteran or User
• Last Name	Last Name of Veteran or User
• Email address	Personal Email Address
• Contract acquisition data Revenue	Fedmine data element
• EnvironmentIdentifier	Environment ID of Acquisition Official
• agencyContract,	Agency(s) of which business has federal contract
• figures	**Data element used between OSDBU and Fedmine**
• Position title	Fedmine data element
• VISN, Office,	VISN of Acquisition Official
• Address,	Address of Veteran or User
• City	City of Veteran
• State	State of Veteran
• Postal Code	Veterans Postal Code
• Provider Id.	Provider Id
• Sec Id	Unique security identifier from IAM Provisioning Service (Security Id)
• Telephone Number	Phone No.
• FedmineModule, UserId	Fedmine Module licensed to Acquisition Official.
• (Guid),	Fedmine data element

• CompanyCertification	Certification listed per Federal Contract
• companyOrg,	**Data element used between OSDBU and Fedmine**
• extentContract,	Identifies length of current and past Federal contracts
• GSAContract,	Identifies if Business has (had) a GSA Contract
• SAM UEI.	Number issued by GSA SAM so business can do the contract with government
• Title of an event	Data element that's transmitted for a particular event
• Date of an event**,**	Data element that's transmitted for a particular event
• Location	Data element that's transmitted for a particular event
• *CompanyName,*	Company Name
• *Event description,*	Data element that's transmitted for a particular event
• *Title,*	Title such as Mr., Mrs., Ms., Dr., or other title
• *IsVerified*	Identifies if business is verified by OSDBU
• *Primary Email,*	Primary Email.
• *Company Type*	Company type
• BondingLevel,	Level Business is Bonded for
• CveVerificationDate,	Date CVE application verified
• YearEstablished,	Year business was established
• EmployeesNumber,	Number of employees
• EmployeesNumberVet,	Number of veteran employees
• IsVeteran	Identifies if business is owned by a Veteran
• IsMinorityOwned,	Identifies if business is minority owned.
• IsServiceDisabled,	Identified if business is verified by OSDBU
• IsWOSB,	Identifies if business is woman owned
• CertifiedCor	Name of certified contracting officer

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.

VEMS powers the Enhanced Vendor Profile (EVP) web application through an interface with Fedmine data mining. EVP provides VA acquisition officials the following functionalities: risk management, goals management, and acquisition analytics tools. The goals management and acquisition analytics are powered by Fedmine. Fedmine will amend the system nightly for businesses with new contract data. Vendors will not have multiple business profile records and individual user profiles will be merged if multiple CSP's are used to log into the VetBiz 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.

If a user requires assistance and contacts an OSDBU program area directly, or the OSDBU Call Center, an interaction record is created and associated with the profile record in question. Approved System Administrators will be afforded access to the CRM

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?

VEMS data in transit uses Transport Layer Security (TLS) which encrypts internet traffic of all types. VEMS data remains secure and available, while adhering to all VA data-protection regulations. Cloud provider security mechanisms are in place and enforceable to protect VEMS PII transactions through Federal Information Processing Standard (FIPS) 140-2 approved data encryption in transit, in use, and at rest.

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

VEMS no longer collects SSN. Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IP.

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

Read access to the system is via internet access, while VA staff, and contractor personnel will have access to the system, via VA Intranet and local connections, for operations, management and maintenance purposes and tasks. Access to the Intranet portion of the system is via VA PIV authentication and role-based access control, at officially approved access points. Veteran owned small businesses will establish and maintain user-ids and passwords for accessing their corporate information under system control using VA's DS Logon, ID.me or Login.gov through Access VA. Policy regarding issuance of user- ids and passwords is formulated in VA by the Office of Information and Technology, Washington, DC. Security for data in the VetBiz database complies with applicable statutes, regulations and government-wide and VA policies.

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?

As VA contractors, Microsoft employees are required to complete basic refresher security awareness training annually at the minimum for access to systems. Access to the Intranet portion of the system is via VA PIV authentication and role-based access control, at officially approved access points. Veteran-owned small businesses will establish and maintain user-ids and passwords for accessing their corporate information under system control using VA's DS Logon or ID.me. Privileged access is only given to administrators via ePASS approval process. Also, VA may disclose information from this system to appropriate agencies, entities, and persons when VA suspects or has confirmed that there has been a breach of the system of records or PII information

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

Access limited to backend use only. System pulls the information that is registered.

2.4c Does access require manager approval?

D365 CRM access requires a license. Need OIT PM approval via SNOW ticket process, limited role

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

Audit function is turned on in CRM & documented. Login name is tracked.

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

ISO, VA OIT PM

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
Middle Name
Suffix
Last Name
Email address
Contract acquisition data Revenue
EnvironmentIdentifier
agencyContract,
figures
Position title
VISN, Office,
Address,
City
State
Postal Code
Provider Id.
Sec Id
Telephone Number
FedmineModule, UserId
(Guid),

CompanyCertification
companyOrg,
extentContract,
GSAContract,
SAM UEI.
Title of an event
Date of an event,
Location
CompanyName,
Event description,
Title,
IsVerified
Primary Email,
Company Type
BondingLevel,
CveVerificationDate,
YearEstablished,
EmployeesNumber,
EmployeesNumberVet,
IsVeteran
IsMinorityOwned,
IsServiceDisabled,
IsWOSB,
CertifiedCor

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.*

OSDBU VIP module of the VEMS system is permanently shut down on 30 DEC 2022, and the functionality is moved to the SBA. As part of the migration of functionality, move also includes all existing VIP module data from the current platform (D365 GCC and SharePoint Online), to the SBA's new platform hosted on AWS. There will be no files collected as VEMS will not be retaining copies of documents going forward. However, until full decommission, currently required artifacts are retained for 7 years and destroyed after the time period . This process will change soon in few months once the D365 is removed. The record schedule and retention policy are as follows; Required artifacts uploaded to a business profile to supplement the verification process have a destruction date of 7 years after completion of the process. Artifacts associated with business profiles whereas the submitter withdraws from process contention are destroyed immediately.

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?

VEMS adheres to the VA RCS DAA-0015-2018-0003 schedules for each category of data it maintains. When the retention data is reached for a record, VEMS carefully disposes of the data by the determined method *3.3b Please indicate each records retention schedule, series, and disposition authority.*

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
https://www.archives.gov/records-mgmt/grs

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.

Records are destroyed using an TRM approved electronic records management application. At the end of the retention period records due for destruction are placed in a digital queue for the responsible records manager, where they are reviewed, and destroyed. A certificate of destruction is produced and kept on file as a result.

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

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

PII is not used during testing or training. Test Veterans with artificial data are used to test the application. Test Veterans are provided by IAM. End-users utilize the same test Veterans during training. Additionally, all training materials display example data using test Veterans. Currently, VEMS data is not used for research. The project team plans to de-identify all data to minimize the risk to privacy when using PII for research

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.

Not Applicable

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Identify and Access Management (SSOe and SSOi) Access VA	Access VA	Last Name, First Name, SecID	Application Program Interface (API)
Active Directory Federation Services (ADFS)	Active Directory Federation Services (ADFS)	VA email address	Application Program Interface (API)

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

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:

<u>Privacy Risk:</u> VEMS requires various information technology skillsets to operate and maintain, ie system administrators, developers, engineers, customer service representatives, etc. Internal access to VEMS by OSDBU personnel does pose a privacy risk due to possible negligence be it willful or inadvertent.

Mitigation: OSDBU access control measures control access to VEMS resources and the type of access permitted. These controls are incorporated into the VEMS operating systems, data base management systems, and applications with higher-level security measures implemented into external devices, such as routers at a VA-approved data center.

Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. VEMS users agree to comply with all terms and conditions of the VA National ROB by signing a certificate of training at the end of the training session.

All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a VA Project Manager. At minimum, the following information should be provided for each VA Project Team member requesting access to the VEMS Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Fedmine	Source of publicly available information about vendor companies	Contract acquisition data Revenue figures Email Fist Name, Last Name, Position title Email, VISN, Office, Address, City, Zip, Phone Number, FedmineModule, UserId (Guid),	MOU - ISA	Application Programming Interface

		EnvironmentIdentifier agencyContract, categoryContract , companyCertification companyContact, companyOrg, extentContract, GSAContract, **SAM UEI**		
My Business Matches	Source of publicly available information to match Government contracts with vendor companies	First Name, Last Name, email address, Organization name, Title of an event, Date of an event, Location Event description. Email, CompanyName, Primary Email, Company Type, Title, City, State, Zip, Phone, NAICS, IsVerified, Address, SecId, BondingLevel, CveVerificationDate, YearEstablished, EmployeesNumber, EmployeesNumberVet, IsVeteran, IsMinorityOwned, IsServiceDisabled, IsWOSB, CertifiedCor, **SAM-UEI**	MOU ISA	Application Programming Interface

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.

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: The risks associated with external sharing information, may affect OSDBU's confidentiality, integrity of information.

Mitigation: In the future, external sharing risks will be mitigated by proper markings on documents; requirements for secure access; and appropriate transmittal mechanisms that vary depending on the nature of the information contained therein, and the vehicle by which it is transmitted.

The CRM Cloud Hosting environment memorializes the agreement between the VA and Microsoft regarding the development, management, operation, and security of a connection between the VA environment and the Infrastructure as a Service (IaaS) environment owned by Microsoft. The MOU-ISA and ISA documents the terms and conditions for sharing data and information resources in a secure manner, defines the purpose of the interconnection, identifies relative authorities, and specifies the responsibilities of participating organizations.

Additionally, OSDBU implemented access control measures to access to VEMS resources, but also the type of access permitted. These controls are incorporated into the VEMS operating systems, data base management, and applications with higher-level security measures implemented into external devices, such as routers at a VA-approved data center

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.

Notice to individuals is covered in SORN for categories of individuals covered by the system, record access & notification procedures. Administrative, Technical and Physical safeguards that's exist for the system is also covered under SORN. Link is provided in Appendix -A 6.1

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.

SORN published in the federal register is tracked here https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08610.pdf

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

Not Applicable. VEMS no longer use the verification form process

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.

Credential and Service Provider like DS Logon and ID.Me provide the name, logon, address and contact details. Vendor may be asked to provide capability statement when registering for direct access events.

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

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

Veterans have the opportunity and right to decline and provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent *is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.*

Credential and Service Provider like DS Logon and ID.Me provide the name, logon, address and contact details. Vendor may be asked to provide capability statement when registering for direct access events

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:

Section 6. Access, Redress and Correction

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

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

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

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

Individuals no longer have access to profile and any profile changes need to go through customer service like VetBiz@va.gov or VEMS Help Desk directly at (866) 584-2344.

Alternatively, individuals wishing to inquire, whether this system of records contains information about themselves, should contact the IT Systems Integration, 810 Vermont Ave. NW, Washington, DC 20420

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).

Not Applicable.

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

Not Applicable.

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.

Individuals can edit inaccurate information, directly via VEMS, by submitting an email to VetBiz@va.gov or they can contact the VEMS Help Desk directly at (866) 584-2344.

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 VetBiz Portal system does allow users listed as the Business Owner to update information, however, there are some fields within the profile that require an update from another source system or require the assistance of a CSR at the Office of Small & Disadvantaged Business Utilization (OSDBU) Call Center. These fields display this information as the user hovers over the fields in the Business Profile form

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

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

group of systems. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals can edit inaccurate information, directly via VEMS, by submitting an email to VetBiz@va.gov or they can contact the VEMS Help Desk directly at (866) 584-2344

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that an individual provides inaccurate or incomplete information that is required to register for OSDBU sponsored events. Accurate information is needed for anyone trying to search for OSDBU programs and services via the VEMS web-portal. VEMS provides these capabilities using a Customer Relationship Management (CRM) platform – Microsoft CRM Dynamics 365 to support OSDBU Business Processes.

<u>Mitigation</u> Users are afforded the capability to log into their VEMS account to view or update their information. They can also contact VEMS support by either the phone or email listed in 7.2.

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.

The VEMS system will serve VA internal and external end-user communities, and three secondary end-user communities. The table below describes the primary VEMS users and their responsibilities. User Level such as Primary and Roles such as General Staff users, and Acquisition Professional, work assignments, produce reports, handle inquiries, and provide insight into business processes research activities, work assignments, produce reports, handle inquiries. Use the system to work assignments, produce reports. Call center agents are responsible for producing reports, handle inquiries and provide insight into business processes.

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?

Users have Full Control or Read only access to data defined by role-based access. OSDBU Managers, Power Users and System/Database Admins are responsible for work assignments, producing reports, handling inquiries, and providing insight into business processes. Power users Modify system configuration, such as configuring business rules, workflows, launch screens, dashboards, alerts, reports, and underlying analytics functionality. System/Database admins focus on maintaining and ensuring optimal performance of the system, configuring connections to new systems in the future, updating the system database. Access level for OSDU Managers include Full Control or Read Only access to data defined by role-based access. Power users have full control and approval but no access to Veteran data. Secondary users such as Non-VA Employee access the system from the public Internet to interact with VA staff, other businesses, or support services. Access level for most secondary users include View Access Only to select subset of data defined by role-based access

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.

Procurement decision makers use the system to process work assignments, produce reports, handle inquiries, and provide insight into business processes. Acquisition Professional use the system to perform market research activities, work assignments, produce reports, handle inquiries, and provide insight into business processes. Procurement decision makers have Full Control to select subset of data defined by role-based access (e.g., procurement, opportunity and event 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.

Office of Small & Disadvantaged Business Utilization (OSDBU) contractors must first be granted a VA clearance and VA network account before we can provide access to the systems. All contractors are required to sign Non-Disclosure Agreements prior to access to the systems.

Contractors are also required to complete VA Privacy/Info Security Training annually. In addition, access must be approved by an authorized federal team lead/supervisor. Contractor access is reviewed monthly by the COR. Contracts are reviewed annually by the COR.

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

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

Personnel 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 as part of the security awareness training which all personnel must complete via the VA’s Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. After the user’s initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training.
Acceptance obtained through electronic acknowledgment is tracked through the TMS system.
All VA employees must complete annual Privacy and Security training. VEMS users agree to comply with all terms and conditions of the VA National ROB by signing a certificate of training at the end of the training session.
All individuals requesting access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a VA Project Manager. To ensure that this requirement is met, the designated Veterans Relationship Management (VRM) Project point of contact (POC) must submit a signed Access Request From for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the VEMS Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or

Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Current*
2. *The System Security Plan Status Date: **07/14/2022***
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 06/30/2022
5. *The Authorization Termination Date:* 06/29/2025
6. *The Risk Review Completion Date:* 05/09/2022
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.***

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)*

Government Community Cloud (GCC) Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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.*

VEMS is hosted within VAEC MS AZURE GOVT & Microsoft AZURE GOVERNMENT (commercial cloud computing environment). This FedRAMP approved, FISMA moderate environment provides Infrastructure as a Service (IAAS) and Software as a Service capabilities to VEMS, such as web and database servers for the various applications that comprise VEMS.VA owns the ownership rights over PII data for VEMS

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.

VAEC MS AZURE GOVT & Microsoft AZURE GOVERNMENT (Common Control Providers) is the hosting environment and provide cloud services such as IaaS, Saas along with a set of common services, security, and connectivity between the cloud environments and the VA network. The providing system collects the ancillary data.

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

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

VA Privacy Service coordinates with Office of Acquisition and Logistics (OAL) and Office of Operations, Security, and Preparedness (OSP) to establish privacy roles, responsibilities, and access requirements for contractors and service providers and includes privacy requirements in contracts and other acquisition related documents. FedRAMP approved, FISMA moderate environment provides Infrastructure as a Service (IAAS) capabilities to VEMS, such as web and database servers for the various applications that comprise VEMS

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).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

TYRONE BROWN

Digitally signed by TYRONE BROWN
Date: 2023.04.07 13:06:32 -04'00'

Privacy Officer, Tyrone Brown

Bernadette Bowen-Welch 111245

Digitally signed by Bernadette Bowen-Welch 111245
Date: 2023.04.07 14:02:08 -04'00'

Information System Security Officer, Bernadette Bowen-Welch

Carol Cleveland 892185

Digitally signed by Carol Cleveland 892185
Date: 2023.04.07 12:26:14 -04'00'

Information System Owner, Carol Cleveland

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).

https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08610.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices