Privacy Impact Assessment for the VA IT System called:

Vendor Event Matchmaking System (VEMMS)

Office of Small and Disadvantaged Business Utilization
VA Corporate

Date PIA submitted for review:

05/03/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tyrone Brown	Tyrone.Brown@va.gov; vharicprivacyofficer@va.gov	202-632-8204
Information System Security Officer (ISSO)	Bernadette Bowen-Welch	bernadette.bowen-welch1@va.gov; vharicisosupport@va.gov	202-461-6894

	Name	E-mail	Phone Number
Information System Owner	Terrill Harrison	terrill.harrison@va.gov	202-461-5468

Abstract

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

The Vendor Event Matchmaking System SaaS provides a digital platform for Federal Acquisition officials to engage targeted socio-economic firms regarding current and future Federal Contracting Opportunities as directed by the Secretary of the VA.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Vendor Event Matchmaking System (VEMMS) is a Software-as-a Service (SaaS) solution owned by the Office of Small and Disadvantaged Business Utilization (OSDBU) that meets High

FedRAMP compliance standards as it is hosted in the Amazon Web Service commercial cloud. The solution provides federal acquisitions officials a platform to engage mandated targeted socio-economic firms (to include but not limited to Veteran Owned Small Business (VOSB), Service Disabled Veteran Owned Small Business (SDVOSB), and minority owned business, etc.) in real time and assess their readiness to provide goods and/or services to the VA and or other Federal Agencies in support of the requirements of Public Law 109-461 which charges OSDBU with the responsibility of verifying eligible firms and facilitating acquisition programs for the aforementioned targeted socio-economic firms. VEMMS is a VA System of Record and will prompt an amendment to SORN 181VAOSDBU.

VEMMS interfaces with the Veterans Information Pages (VIP) business system, and the VetBiz Portal. The interface with VIP is an Application Program Interface (API) that provides public profile data on registered verified veteran owned firms as well as registered large and small commercial businesses. while the VetBiz Portal provides authentication via an SSO to allow system access to users.

The system database stores both publicly available and personal profile data on approximately 5000 registered firms, firm representatives, and acquisition officials. Contact information for acquisition officials are not viewable to event participants.

The VA is the owner of all data within VEMMS the contract specifically states that no information made available for performance shall be used only for the purposes listed therein and shall not be used in any other way without expressed written consent of the VA. Data within VEMMS may not be used for any purpose outlined within the parameters of the contractual agreement unless written permission is given by the System Owner or requested via court order. A large portion of the data contained with the system is public, PII data includes email addresses, phone numbers, and listed business addresses therefore minimal impact to the reputation of the CSP would or its customers would result should data within contained within be disclosed. The system will be utilized per the conditions

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 Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

- Business Email
- Company/Organizational Name
- Company Address
- Company City
- Company Zip
- Company State/Province
- Company Country
- Company Phone
- Company Website URL
- Salutation
- First Name
- Last Name
- Position
- Business Cell Phone
- Registration Email
- Product Service Code

- Profile Photographs
- Industry
- Year Business was established
- Data Universal Numbering System DUNS®
- Business Type
- Highest Level of Personal Security Clearance
- Do you have a Defense Contract Audit Agency Compliant Account
- Defense Contact Audit Agency number (optional)
- Core Competency/Strength
- CVE Verification Expiration Date
- Are you currently doing business or have a contract with the VA? (Yes/No)
- Have you had a contract with the VA in the last 5 years? (Yes/No)
- Government Category
- Socio-Economic Category
- Certifications
- Federal Supply Contracting Vehicle
- States in which you do Business

PII Mapping of Components

VEMMS consists of 1 key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VEMMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

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
VEMMS Database	Yes	Yes	First Name, Last Name Email Address	Required for the establishment of user profiles to register for VA acquisition events	In accordance with 6500 Handbook (Privacy and controls) Integration with VA Access VA CSP (DS Login, id.ME, and PIV) Role based access

					and least privilege principals have been incorporated

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

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The sources of information for VEMMS include the Veterans Enterprise Management System-Customer Relationship Manager (VEMS-CRM) database as the single source of truth, however, users may amend sections of their profile data that has not been pulled via the API. Any sections of user profile data that has been pulled via the API will be static and will require direct engagement with the OSDBU program area that verifies the data in question.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Any firm that wants to be considered for the Vets First acquisition awards must submit an application for review. Users are aware that this data is used to conduct market research for acquisition award. Verified firm profile data is collected via an encrypted API from VIP and initially placed on a form within VEMMS to allow the user to confirm the accuracy of the data on their VEMMS dashboard.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Any profile data provided via the API from the VIP-CRM web service cannot be changed by the VEMMS user. Any previous profile that may have been created prior to the integration of VEMMS into the VEMS system will be overwritten using the VEMS-CRM data as it is the single source of truth with the profile username being the unique reference ID. The username will mirror the email address listed on the user's individual contact record within VEMS-CRM.

Users will have read only access to data that has been pulled through the API from VIP-CRM. If data provided via the VIP-CRM API is reviewed by the user and requires amendment, the user must engage the OSDBU Center for Verification or access their VIP account directly to make changes to the data in question. Data pulled via the API from VEMS-CRM may overwrite profile data within VEMMS. All APIs are encrypted during transit using SSL technology.

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 VEMMS application complies with and supports the following federal regulations and/or departmental policies and guidelines;

• 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
• VHA Directive 2009-021 Data Entry Requirements for Administrative Data
• OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000
• Pub. L. 108–183 (December 2003), the Veterans Benefits Act of 2003, Sections 301, 305, 308.
• Pub. L. 106–554 (December 2000), Sections 803 and 808.
• Pub. L. 106–50 (August 1999), the Veterans Entrepreneurship and Small Business Development Act of 1999.
• Pub. L. 105–135 (December 1997), Title VII, Service Disabled Veterans Program.
• Pub. L. 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.

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: It is possible for users to update editable sections of their profile with non-public PII data.

Mitigation: A disclaimer is provided to users during the event registration workflow that they should not include PII such as personal addresses, phone numbers, financial account numbers, and/or SSNs to their profiles. The API interface with VIP-CRM does not pull any non-public PII data during the call.

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.

Business Email	Used to Contact Individual and establish profile
Company/Organizational Name	Used to Contact Individual and establish profile
Company Address	Used to Contact Individual and establish profile
Company City	Used to Contact Individual and establish profile
Company Zip	Used to Contact Individual and establish profile
Company State/Province	Used to Contact Individual and establish profile
Company Country	Used to Contact Individual and establish profile
Company Phone	Used to Contact Individual and establish profile
Company Website URL	Used to Contact Individual and establish profile
Salutation	Used to Contact Individual and establish profile
First Name	Used to Contact Individual and establish profile
Last Name	Used to Contact Individual and establish profile
Position	Used to Contact Individual and establish profile
Cell Phone	Used to Contact Individual and establish profile
Registration Email	Used to Contact Individual and establish profile
PSC	Used to establish profile
Photo	Used to enhance profile (Optional)
Industry	Used to establish profile
Year Business was established	Used to establish profile
Data Universal Numbering System DUNS®	Used to establish profile
Business Type	Used to establish profile
Highest Level of Personal Security Clearance	Used to establish profile
Do you have a Defense Contract Audit Agency Compliant Account	Used to establish profile
Defense Contact Audit Agency number (optional)	Used to establish profile

Core Competency/Strength	Used to establish profile
CVE Verification Expiration Date	Used to establish profile
Are you currently doing business or have a contract with the VA? (Yes/No)	Used to establish profile
Have you had a contract with the VA in the last 5 years? (Yes/No)	Used to establish profile
Government Category	Used to establish profile
Socio-Economic Category	Used to establish profile
Certifications	Used to establish profile
Federal Supply Contracting Vehicle	Used to establish profile
States in which you do Business	Used to establish profile

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

VEMMS provides reporting capabilities to event administrators only. These reports include but are not limited to the following: host, participant/supplier, attendees', meeting, business categories, activities/session, and event tickets purchased. The reporting capability is only available to administrative system users. This capability does not create a separate record it only provides a quantitative analysis of current event and system data.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit 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?

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Data is protected in transit using a FIPS-140-2 compliant VPN encryption tunnel. Physical protection of data is protected at rest using a shared responsibility model with AWS providing a fully managed infrastructure (IaaS) for hosting web applications. This includes but is not limited to the AWS Network firewall. The AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service. Network Firewall is supported by AWS Firewall Manager. AWS Key Management Service (KMS) is a managed service help to create and control customer master keys (CMK's) that use the Advanced Encryption Standard (AES) algorithm. AWS KMS is also integrated with CloudTrail to log use of CMKs for auditing, regulatory and compliance needs.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

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.

Access to PII is limited by the VEMMS application to only those data items deemed necessary for VA Staff to perform their duties. The System Owner is responsible for assuring PII is safeguarded within VEMMS. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII, as well as how it is to be used. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by OSDBU supervisors. User access is provided by OSDBU System Administrators following receipt of request from appropriate individuals. The VEMMS application implements auditing which tracks user access to the system and all data accessed. OSDBU ensure the practices stated

in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

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

- Business Email
- Company/Organizational Name
- Company Address
- Company City
- Company Zip
- Company State/Province
- Company Country
- Company Phone
- Company Website URL
- Salutation
- First Name
- Last Name
- Position
- Cell Phone
- Registration Email
- PSC
- Industry
- Year Business was established
- Data Universal Numbering System DUNS®
- Business Type
- Highest Level of Personal Security Clearance
- Do you have a Defense Contract Audit Agency Compliant Account
- Defense Contact Audit Agency number (optional)
- Core Competency/Strength
- CVE Verification Expiration Date
- Are you currently doing business or have a contract with the VA? (Yes/No)
- Have you had a contract with the VA in the last 5 years? (Yes/No)
- Government Category
- Socio-Economic Category

- Certifications
- Federal Supply Contracting Vehicle

States in which you do Business

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The only records kept in the VEMMS system are the following: photograph, company brochure, company logo, capability statement.

These records are retained for as long as the user has a profile in VEMMS.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

VEMMS is a sub-application of the Veterans Enterprise Management System (VEMS), as such it will adhere retention schedule (DAA-0015-2018-0003), approved April 23, 2020 and published on Federal Register Vol 85, No 79, Pages 22798-22801

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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 Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008). When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports.

The VEMMS application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the VEMMS application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws.

This system does not use paper records.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Training data is located within the Non-production and is not accessible to users external to the VA; Also, any users accessing the Non-Production environment must be an approved system administrator and granted access by the System Owner. The training data is dummy data and does not consist of any PII or PHI.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk: If data is maintained within the VEMMS application for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation: The VEMMS application only retains information necessary for the purpose of allowing users to register for events and match acquisition requirements with the business capabilities of potential business partners. Program Areas within OSDBU are the primary users of the system. They are consulted quarterly in regard to what information is required that will allow acquisition officials to appropriately evaluate the aforementioned business capabilities. Though some of the information for the businesses are considered PII, all data within the system is readily available public data. Irrelevant data is purged via the connection to VEMS-CRM. Verified firms with profile data within VEMMS is overwritten by any new data pulled from the organizations VEMS-CRM profile.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Small & Disadvantaged Business Utilization (OSDBU)/ Vendor Information Pages (VIP) (VEMS-CRM)	Information is submitted on web forms in VEMMS. OSDBU uses the basic user information and company information in support of OSDBU's mission including Center for, Strategic Outreach and Communications, Contracting and Acquisition Support, and Direct Access Programs.	• Business Email • Company/Organizational Name • Company Address • Company City • Company Zip • Company State/Province • Company Country • Company Phone • Company Website URL • Salutation • First Name • Last Name • Position • Cell Phone • Registration Email • PSC • Industry • Year Business was established • Data Universal Numbering System DUNS® • Business Type • Highest Level of Personal Security Clearance • Do you have a Defense Contract Aud Agency Compliant	Data is transmitted via SSL/TLS, and utilizes OAuth 2.0 authentication

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*
		Account? • Defense Contact Audit Agency numb (optional) • Core Competency/Strength • CVE Verification Expiration Date • Are you currently doing business or have a contract with the VA? (Yes/No) • Have you had a contract with the VA in the last 5 years? (Yes/No) • Government Category • Socio-Economic Category • Certifications • Federal Supply Contracting Vehicle • States in which you do Business	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: VEMMS requires various information technology skillsets to operate and maintain, i.e. system administrators, developers, engineers, customer service representatives, etc. Internal access to VEMMS by OSDBU personnel does pose a privacy risk due to possible negligence be it willful or inadvertent.

Mitigation: To ensure business continuity and minimize potential damage due to unauthorized internal access, OSDBU maintains role-based access control to protect PII, other sensitive information, and proprietary information from intentional or accidental disclosure, modification, erasure, or copying, as well as IT resources from misuse. OSDBU access control measures control access to VEMMS resources and the type of access permitted. These controls are incorporated into the VEMMS 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***
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: Not Applicable

Mitigation: Not Applicable

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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.
This question is 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.

VEMMS users are provided notice, guidelines, and instructions on the collection and use of information required for the use of the VEMS. Those notices, guidelines and instructions include the following under SORN 181VAOSDBU:
https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf,
https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08610.pdf & Verification Application Instructions

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

Users are notified that during registration of minimum information required to establish an VEMMS profile. Individuals have the right to decline to provide said information, however, failure to provide requested information can results in the inability to

1) Establish a user profile in VEMMS
2) Meet criteria requirements set by event acquisition officials

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

Users submit all their own information to the system for explicit use by the system. The VEMMS database is an extension of the VIP database that must be made available to all Federal departments and agencies to reach targeted contracting goals established by the Secretary of Veterans Affairs, per 38. USC Title 38 Part VI, Chapter 81, Sub-Chapter II, Sec 8127. Data will not be used outside of the scope.

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.

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: User not provided sufficient notice of uses of private data. User information is not used for purpose in which notice was provided either directly to the individual or through public notice

Mitigation: Users are notified with a pop-up message clearly articulating privacy guidelines upon entering the system. Contractual obligation states the system may only be used for initial intended purpose as directed by the VA. Any other use required expressed written consent from the VA.

Section 7. Access, Redress, and Correction

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

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

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals with the appropriate authentication credentials may access their VEMMS business profile at any time during the retention period via the Vetbiz Portal at https://vetbiz.va.gov/. Select the Event's listing, select the "Login to Events Dashboard" button to authenticate into the VetBiz Portal. The user will be redirected to Access VA for authentication, and later redirected back to the VetBiz Portal as an authenticated user. The Event's listing "Access Event's Dashboard" should now be available. The users will click the button to be redirected to the VEMMS Dashboard and may update certain parts of their business profile by selecting the arrow next to their name on the upper right side of the window.

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.

7.2 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 verificationfollowup@va.com or vems@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.

VEMMS does allow users to update information, however, there are some fields within the profile that require an update from the Vendor Information Pages-CRM system. These fields display this information as the user hovers over the fields in the profile form. Users are notified that they need to contact the OSDBU Help Desk or the OSDBU Center for Verification for assistance via a pop-up message that appears when attempting to edit the data field.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

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

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.

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

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

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

Follow the format below:
Privacy Risk: There is a risk that an individual provides inaccurate or incomplete information that is required to verify eligibility of a VOSB or SDVOSB consequently inaccurate information could be passed to VEMMS via the API.

Mitigation: Users are afforded the capability to log into their VIP-CRM 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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

User Level	Role	Responsibilities	OSDBU IT Capabilities Access Level
Primary	VA Acquisition Officials	Use the system to market small business opportunities to SDVOSBs and VOSBs	View Only access to public data available on small business profiles.
Secondary	Power users	Modify system configuration, such as configuring business rules, workflows, launch screens, dashboards, alerts, reports, and underlying analytics functionality	Full Control, Approval
Secondary	System administrators	Maintaining and ensuring optimal performance of the system, configuring connections to new systems in the future, updating the system database	Full Control, Approval
Secondary	Small-Business Owner or Representative	Access the system from the public	View Access Only to PDM presented

		Internet to submit applications and view status, to view verified businesses, to interact with VA staff, other businesses, or support services	opportunities per event.
Secondary	Commercial Businesses - Authorized receivers of public verification data	Access the system from the public Internet to view verified businesses, to interact with VA staff, other businesses, or support services.	View Only access to public data available on small business profiles
Secondary	States, Local, or Federal Government - Authorized receivers of public verification data and select sensitive data	Access the system from the public Internet to view verified businesses, to interact with VA staff, other businesses, or support services Could view public and select sensitive data	View Only access to public data available on small business profiles

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.

Contractors will have access to publicly available PII on VOSBs and SDVOSBs. Contractors will be responsible for the Operations & Maintenance of VEMMS. Contract is reviewed annually at a minimum. Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task

order. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

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 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 VEMMS 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?

If Yes, provide:

1. *The Security Plan Status,*
2. *The 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).*

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

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

ATO in progress through DTC; categorized at Low

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).

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.

Yes. The system uses cloud technology. There is no current ATO/FedRAMP Authorization for the VEMMS solution on the application level, however this effort has been initiated. The application has been categorized and is currently hosted in the Amazon Web Services East environment. This Cloud Service Provider has an approved FedRAMP Authorization that can be leveraged. The system has a current data security categorization of Low from the VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office. The VEMMS is a Software as a Service.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

There is no contractual agreement between the VA and the CSP. The agreement is between the VA and the SaaS solution vendor My business Matches. However the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is 36C10B19C0029.

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

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

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

The CSP does collect ancillary data like logs, audit trails, profile updates, uploaded files meta data, email sent confirmation, browser data, incorrect login attempts users session. This data belongs to the vendor but is available to the VA upon request.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The selected CSP inherits the following controls from FEDRamp - Authorized Cloud Infrastructure Provider (Amazon Web Services) that includes:

- Physical and Environmental controls
- Patch Management (on infrastructure level)
- Configuration Management (on infrastructure level)
- Awareness & Training (on infrastructure level)

Service Provider (Amazon Web Services) claims responsibility for protecting the hardware, infrastructure software, networking, and facilities that run AWS Cloud services.

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

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

The system does not use 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**

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 provided in this Privacy Impact Assessment is true and accurate.

TYRONE BROWN

Digitally signed by TYRONE BROWN
Date: 2022.05.10 08:56:58 -04'00'

Privacy Officer, Tyrone Brown

Bernadette Bowen-Welch 111245

Digitally signed by Bernadette Bowen-Welch 111245
Date: 2022.05.11 13:51:12 -04'00'

Information Systems Security Officer, Bernadette Bowen-Welch

Terrill N. Harrison 1079525

Digitally signed by Terrill N. Harrison 1079525
Date: 2022.06.02 15:39:59 -04'00'

Information Systems Owner, Terrill Harrison

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

Verification Application Instructions

https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf