Privacy Impact Assessment for the VA IT System called:

electronic Virtual Assistant (e-VA)

Veterans Benefit Administration (VBA)

Veteran Readiness and Employment

Date PIA submitted for review:

08/29/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.Dixson@va.gov	(202) 461-9477
Information System Security Officer (ISSO)	Brian Kohler	Brian.Kohler@va.gov	(412) 822-3272
Information System Owner	Linda Ritchie	Linda.Ritchie@va.gov	(202) 461-9600

Abstract

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

The electronic Virtual Assistant (e-VA) is an active Artificial Intelligence enabled application that alleviates the burden of compliance, data entry, communications, documentation, and repetitive tasks in order to enable VR&E resources to focus their time on Veteran participant's needs, fulfilling the organization's mission of guiding clients to successful outcomes.

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 VA is charged with providing assistance to Veteran Readiness & Employment (VR&E) program participants with service-connected disabilities through VR&E services. The VR&E program is embarking on a transformative modernization which will include a suite of technological advancements, including the use of artificial intelligence (ex. e-VA), to achieve the organization's digital and paperless goals.

electronic Virtual Assistant (e-VA) application is a COTS product purchased from The Career Index (TCI) by the Veteran Readiness & Employment (VR&E) Business Line, which is the legal authority for this system. The System of Record Notice SORN ID is Compensation, Pension, Education, and Veteran Readiness and Employment Records—(58VA21/22/28) and is located at: https://www.oprm.va.gov/privacy/systems_of_records.aspx. VR&E retains ownership rights to the data collected

from the Veterans and from the e-VA system**,** and is responsible for the security and privacy of the data held by the vendor. There will be information sharing with the VBA Corporate Database only.

e-VA is an active Artificial Intelligence (AI) enabled application that alleviates the burden of compliance, data entry, communications, documentation, and repetitive tasks in order to enable VR&E resources to focus their time on Veteran participant's needs, fulfilling the organization's mission of guiding clients to successful outcomes. The primary objective for implementing e-VA is to provide virtual support services that will alleviate administrative tasks from Vocational Rehabilitation Counselors (VRCs). Achieving this objective will allow VRCs to focus on providing world-class service to program participants. e-VA is the first AI-based solution focused on applying these autonomous capabilities to the complex field of human services.

The VA has authority to provide all services and assistance necessary to enable eligible Veterans with service-connected disabilities to obtain and maintain suitable employment and, if not employable, achieve independence in daily living to the maximum extent feasible. To accomplish this, the VA has a contract (#36C10E19P0165) with the Commercial Off The Shelf (COTS) vendor, The Career Index (TCI), for the e-VA system application. As part of this contract, the VA has acquired 1,200 user licenses from TCI for the VR&E counselors. The VA retains ownership rights to the data generated by the application. VR&E processed over 112,848 applicants in FY19. At the end of FY19, there were 122,249 enrolled VR&E program participants and the number of enrolled participants continues to rise.

Features of this e-VA application:

- Supports bi-directional electronic communication between the e-VA application and VR&E staff, and between the e-VA application and VR&E program participants, as native functionality within the provided software.

- Provides the capability for documents and images to be uploaded by program participants either through SMS text messaging or email from their mobile device, such as training certificates, training receipts, or employment verification documents.
- Enables system-generated, interactive appointment scheduling, rescheduling and cancellation with the program participant.
- Provides announcements and broadcast messages to an ad-hoc set of users and program participants.
- Facilitates bi-directional data integration between e-VA application and VA systems, specifically the VBA Corporate Database.

The e-VA solution shall adhere to the following VA guidelines:

- It is hosted and managed within FedRAMP-certified AWS cloud environment, owned by the vendor.
- It will communicate bi-directionally with VA systems only via existing authorized trusted internet connection (TIC).

The e-VA COTS application and database is hosted as a Software-as-a-Service (SaaS) configuration in a vendor-owned (non-VA) Amazon Web Services (AWS) GovCloud environment, utilizing a Virtual Private Cloud (VPC). This application instance is only used by the VA and thus is single-tenant. Each AWS VPC is completely segregated from other VPCs hosted on the AWS GovCloud with no way to move information or applications from VPC to VPC. The rest of the e-VA system components are VA custom- developed and are hosted in a VA Enterprise Cloud (VAEC) VPC, which resides in a VA-owned AWS GovCloud VPC. The vendor's AWS GovCloud VPC and the VAEC GovCloud VPC do not have overlapping boundaries.

The e-VA application, residing in the vendor-owned AWS GovCloud has three (3) separate communications connections.

Communications Connection #1 (C1):

- **Who/what uses this connection?** The e-VA application will be available to all VR&E Counselors in the VA Central Office (VACO), 56 Regional Offices (ROs), National Capital Region Benefits Office (NCRBO) and approximately 300 out-based locations throughout the Continental United States (CONUS), Alaska, Hawaii, the Philippines and Puerto Rico, who have been granted access by his/her supervisor.
- **What PII is transported over this connection?** Refer to Section 1. Characterization of the Information for PII details.
- **How is the PII protected on this communications connection?** An SSL certificate has been generated for this connection which provides authentication for the e-VA application and enables an encrypted connection. The e-VA application is accessible by the users (Counselors) from the VA network by entering an external URL in the user's browser, using Government-furnished equipment (GFE) or other controlled methods of accessing the VA Network, including the Citrix-Access Gateway (CAG) services via two-factor PIV-enabled access. The user must log into the application, using PIV authentication or userID and password that has previously been set up by an assigned Administrator of the e-VA application.

Communications Connection #2 (C2):

Who/what uses this connection? The e-VA application will communicate bi-directionally with the VBA Corporate Database to perform the following two functions:

- Participant Case Notes will be sent from the e-VA cloud application and written into the VBA Corporate Database.
- Updated/New Participant information queried nightly from the VBA Corporate Database will be sent to the e-VA cloud application.

- **What PII is transported over this connection?** Refer to Section 1. Characterization of the Information for PII details.
- **How is PII protect on this communications connection?** A unique SSL certificate has been generated for this connection which provides authentication for the e-VA application and enables an encrypted connection. The connection will use HTTPS protocol, which is a secure connection and the e-VA application will only accept communications on a specific port and from a specific VA IP address.

Communications Connection #3 (C3):

- **Who/what uses this connection?** Veteran email addresses and cell phone numbers used by this application are retrieved from the VBA Corporate Database (VBA's database of record for Veterans). This information is gathered and/or verified during the VR&E program eligibility process and stored in the VBA Corporate Database. Prior to the initial communication by the application, the participant does not have any way of communicating with the e-VA application. When the VRC initiates the first program assignment for the participant (no PII included or requested), the e-VA application will send an introductory text message, which includes a link to the e-VA Terms of Service and Privacy Policy. These Terms warn the participant not to send PII over this channel at any time or for any reason. The participant must "accept" these Terms to opt in to continue communicating with the e-VA application. These automated communications include scheduling counseling appointments, receiving updates on current assignment and new assignments. In the same introductory text, the participant has the opportunity to correct their email address and to choose their preferred method of communication (text or email). Once the initial communication from the e-VA application is received, the participant has the capability to initiate a text or email to the e-VA application, using the Short Code from previous system texts or the e-VA's email address. In either case, the e-VA application stores the text or email in the participant's Case Note record and sends an alert to the assigned VRC to respond to the participant. There is no website, link or dashboard in this e-VA application accessible by the program participant.
- **What PII is transported over this connection?** Refer to Section 1. Characterization of the Information for PII details.
- **How is PII protect on this communications connection?** A unique SSL certificate has been generated for this connection which provides authentication for the e-VA application and enables an encrypted connection. Short Message Service (SMS) text messages are processed using a secure SMS gateway hosted by Twilio. The client's first and last name (the only PII in the text message) are encrypted when the information is passed back and forth.

Outbound emails to the program participants are routed by the e-VA application in the vendor GovCloud over the Business Partner Extranet (BPE) secure connection to the VA's partner SMTP server. The email is then sent through the TIC Gateway over the public internet to the participant. All emails to participants are sent from a single email address (eva@eva.va.gov).

Inbound emails from the program participant are routed through the VA's TIC Gateway, processed and then sent over the BPE connection to the e-VA application.

The VA instance e-VA COTS application will only reside in their vendor-owned AWS GovCloud (one site). The PII stored in the AWS GovCloud will be first/last name, email address and cell phone which will be updated nightly via a batch job querying the Corporate Database (source data store).

This Privacy Impact Assessment (PIA) will not result in circumstances that require changes to business processes, nor require any technology changes.

Legal Authorities for this system are:

- National Archives and Records Administration (NARA) (44 U.S.C Chapter 21) c 2102 (a) (Pub. L. 98-497, § 103) (a)
- Records Management by the Archivist of the United States (44 U.S.C. Chapter 29) c 2901 .2 "Record Management; c 2605 (a) "Selective Retention of records; security measures.
- VA Directive and Handbook 6502, Privacy Program
- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) between VA and Halfaker*
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- Federal Information Security Management Act (FISMA) of 2002
- The System of Record Notice (SORN) ID is Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—(58VA21/22/28) at the following link: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

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)

- Unique internal participant ID

PII Mapping of Components

The e-VA system consists of (1) key components, including the Corporate Database. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by e-VA and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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.

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
			•		
Corporate Database	No	Yes	• Name • Personal Phone Number • Personal Email Address	Case Notes from the e-VA application	• Storage of this data is inside the VA network. • PIV card must be

			• Unique internal participant ID		used to log into the VA network. • Access to the Corporate Database is restricted to those users who require access and must be approved by the employee's manager or the Contracting Officer Representative (COR) of the project.

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 data that will support e-VA originates from the VA's VBA Corporate Database (CorpDB), a central enterprise-class Oracle relational database that is the system of record for VBA benefits data. The information from CorpDB that identifies VR&E Veteran participants shall be interfaced with e-VA via the supplied synchronization utilities. Regular updates will be bi-directionally interfaced through the same utilities on a near-real-time scheduled basis.

Information that is sent to the e-VA application via the NSOC-approved Trusted Internet Connection (TIC) will include:

- Participant identifiers
- Participant e-mail address
- Participant cell phone number
- Unique internal participant ID
- Unique internal staff ID associated with the participant
- Case Status (i.e., application, job search, etc.)
- Date that status was entered

The e-VA application will also be collecting information from the participant as requested by the VRC, such as training certificates and employment verification via their mobile device. The participant will be warned not to send any documents with PII, other than first/last name. These images will be stored in e-VA's database in AWS GovCloud. The e-VA application will also be producing Case Notes on each participant. These will be stored in the Corporate Database.

Feedback Collection

Given the many methods in which Veterans engage with VA, it is important that VA has the ability to collect feedback and data via the different touchpoints, channels, and devices that veteran participants will use. The major touchpoint that e-VA will offer include, two-way texting, and email to automatically gather key performance and progress information from participants. Refer to section 1.3 for encryption mechanisms for email and texting. All e-VA modalities comply to all mandated VA security requirements and are compatible for desktop, tablet, and mobile devices. The data collection mode utilized shall at the time of requirements definition, shall be delivered based on factors such as the participants preferences, the desired information and materials to be collected, the volume of data to be collected, and the measures and metrics required to achieve the VA's desired outcome.

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.

e-VA reaches out to participants to collect progress and case status information using several modalities (NOTE: e-VA does not allow for participants to query their profile, case status or any other kind of information retrieval):

Feedback Collection Modes	Description
Two-way Texting	**e-VA allows for two-way texting in order to communicate with the participate. The participant can confirm appointments with the Counselors, answer interview questions, and provide information, such as training certificates, employment verification documents and training receipts e-VA includes natural language processing in order to understand answers coming back from participants.** **Short Message Service (SMS) text messages are processed using a secure SMS gateway hosted by Twilio. The client's first and last name (the only PII in the text message) are encrypted when the information is passed back and forth.**
Email	**e-VA uses email messages with embedded link to the data collection records specifically prepared for the participant in the e-VA database. The encrypted link includes three unique, numeric pointers that informs the application who the participant is, who the case manager is and a hash value that are checked against the e-VA data store before the interview is commenced by the web data collection application.** **Outbound emails to the program participants are routed by the e-VA application in the vendor GovCloud over the Business Partner Extranet (BPE) secure connection to the VA's partner SMTP server. The email is then sent through the TIC Gateway over the public internet to the participant. All emails to participants are sent from a single email address (eva@eva.va.gov).** **Inbound emails from the program participant are routed through the VA's TIC Gateway, processed and then sent over the BPE connection to the e-VA application.**

NOTE: VA Participants are informed about the e-VA services via letter from the VA VR&E Division (existing participants) or as part of the VA VR&E eligibility process (new participants). The information includes what the e-VA application is and what it does, how e-VA will communicate including the email address and cell phone number the application will be using as well as instructions on how to opt out. The first message from e-VA to any participant is always the opt-in/opt-out message. If the participants opts out, e-VA will not continue any further communications to the participant using the opted-out connection, unless the participants later specifically opts in.

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.

Information that is collected and/or generated by e-VA shall occur as a combination of data entry that occurs through the various methods described above and application interfaces.

During data entry via the e-VA user interface, errors cannot be ruled out entirely due to the various freeform and uncontrolled data entry fields that will be presented to veteran participants. However, e-VA assumes that errors in data will occur and present various input validation tests to prevent erroneous data from being processed and stored. Standard input validation addresses common data entry errors including; missing data, incorrect field lengths, data having unacceptable composition, dates are out of range, dates are invalid, data do not match stored data.

When feasible, data entry input transaction into e-VA are validated through a variety of common techniques, including validation against system of record details via application program integration (API). Common data validation checks include but are not limited to; missing data test, field length test, class or composition test, reasonableness and range test, invalid values test, cross-reference tests, string values tests, and check-digit and self-validating tests.

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

- National Archives and Records Administration (NARA) (44 U.S.C Chapter 21) c 2102 (a) (Pub. L. 98-497, § 103) (a)
- Records Management by the Archivist of the United States (44 U.S.C. Chapter 29) c 2901 .2 "Record Management; c 2605 (a) "Selective Retention of records; security measures.
- VA Directive and Handbook 6502, Privacy Program
- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) between VA and Halfaker*
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- Federal Information Security Management Act (FISMA) of 2002
- System of Record Notice (SORN) is Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—(58VA21/22/28).

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: Sensitive Personal Information (SPI) including personal contact information, may be released to unauthorized individuals.

Mitigation: Profile-based permissions will govern what participant information the data users will be able to access. The profiles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to participant's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

Privacy Risk: Unsecured Sensitive Personal Information (SPI) including personal contact information, may be exposed.

Mitigation: To mitigate this risk, e-VA protects data by ensuring that only authorized users can access it. Data security rules are assigned that determine which data users can access. User access is governed by VA password security policies, using PIV cards. The connection used by the authorized users to access the e-VA application uses HTTPS secure protocol. The e-VA application only accepts data traffic from a specific range of VA IP addresses. All other traffic is ignored by e-VA. Participant name is stored encrypted using triple des algorithm with 128 key bit length. All passwords are stored in Secure Hash algorithm (SHA) 256 one-way hash format.
Privacy Risk: Data breach at the facilities level.

Mitigation: To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the e-VA system rooms/cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

Privacy Risk: Data breach at the network level.

Mitigation: Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on ports 80 and 443, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls point of entry.

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.

- First/Last Name – used as an identifier
- Email Address – used to contact the program participant
- Cell phone Number – used to contact the program participant
- Unique internal participant ID – used as an identifier

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

e-VA's primary data analytics tools are dynamic reports that are used by staff to isolate potential participant issues as well as management reports that are used to determine which staff needs support, training and/or enforcement.

As this point, e-VA is not using analytic tools beyond standard reporting.

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

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. e-VA is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology, employees such as VR&E counselors who are responding to the participants have each undergone extensive background checks and has taken the required annual privacy training, as well as signed off on Rules of Behavior document.

The System of Record Notice SORN ID is Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—(58VA21/22/28) and is located at: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Access to the participant information is determined by their Manager's approval. There will be assigned Administrators of this application at the Regional Office level, who will have access to create/change/delete user permissions, based on manager's written approval. VA users will be required to use their PIV card as their primary access to the application. A backup access will be via VA user ID and password. Based on their login credentials, the VA users will only have access to information on those participants to which they are assigned by their Manager. Any entry into the application for a participant will be logged with the user's userID making to change. The e-VA application resides in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. The VBA Corporate Database is owned and maintained by VA ITOPS, who ensures data security.

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:

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. e-VA is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology, employees such as VR&E counselors who are responding to the participants have each undergone extensive background checks and has taken the required annual privacy training, as well as signed off on Rules of Behavior document.

The System of Record Notice SORN ID is Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—(58VA21/22/28) and is located at: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Access to the participant information is determined by their Manager's approval. There will be assigned Administrators of this application at the Regional Office level, who will have access to create/change/delete user permissions, based on manager's written approval. VA users will be required to use their PIV card as their primary access to the application. A backup access will be via VA user ID and password. Based on their login credentials, the VA users will only have access to information on those participants to which they are assigned by their Manager. Any entry into the application for a participant will be logged with the user's userID making to change. The e-VA application resides in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. The VBA Corporate Database is owned and maintained by VA ITOPS, who ensures data security.

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/Last Name
- Personal Email Address
- Personal Cell Phone Number
- Unique internal participant ID

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 e-VA system is designed to gather VR&E Veteran Participant data that is analyzed and managed in order to drive actionable outcomes pursuant to Title 38 USC Chapters 18, 31, 35 and 36, to provide all services and assistance necessary to enable eligible Veterans with service-connected disabilities to obtain and maintain suitable employment and, if not employable, achieve independence in daily living to the maximum extent feasible.

e-VA operates using a combination of batch data feeds, real-time data service calls, and internal databases. e-VA also provides integration components to support bi-directional communication to/from the VBA Corporate Database and the e-VA application. Records retention within the application and the hosted environment is managed, based on the VA's data retention policies.

Records management within the Department of Veterans Affairs is governed by VA Directive 6300, Records and Information Management with specific records management procedures documented in VA Handbook 6300.1. At this time, data collected and maintained by the e-VA shall not be deleted from the system. The purpose of this indefinite data retention is to be able to collect history that will be utilized for analytical trending and program-on-program comparative analysis.

During the period where the retention of data is indefinite, standard operational data management capabilities will be implemented in the form of daily back-up of databases and batch data files to offline storage within the Amazon Web Services Simple Storage Service (S3), through the use of S3 Lifecycle Management rules which describe object lifecycle parameters that are created within the S3 offline storage buckets. The lifecycle configuration consists of one or more rules, where each rule defines and action for Amazon S3 to apply to one or more objects. Object lifecycle rules currently maintain offline backups with no expiration for a period of 60 days. Following 60 days, objects will be transitioned to S3 Glacier storage, which is secure, durable, and low-cost

cloud storage, configured as an integral component of the e-VA application Government Cloud instance, for data archiving and long-term backup.

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.

e-VA complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the e-VA GovCloud instance will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). e-VA records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

The records being retained in the e-VA AWS cloud application are the PII listed in the section above:

- First/Last Name
- Personal Email Address
- Personal Cell Phone Number
- Unique internal participant ID
- Unique internal staff ID associated with the participant

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

e-VA complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Participant data is never deleted in e-VA. If staff "deletes" a record, a delete flag is set which makes the record invisible, but it is never deleted. e-VA backups follow a standard grandfather- father-son schema with daily incremental backups and weekly full backups on a monthly rotation. Each month's backup is archived.

If required, the VA could export the data stored in e-VA and retain it locally in order to meet VA/NARA retention requirements. This is not currently being planned. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given.

When hard drives and backups are at their end of life, the media is sanitized based on GovCloud Media Disposal Policy. Hard drives are overwritten using a multiple--pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Object lifecycle rules currently maintain offline backups with no expiration indefinitely. Objects may be transitioned to S3 Glacier storage, which is secure, durable, and low-cost

cloud storage, configured as an integral component of the e-VA GovCloud instance, for data archiving and long-term backup

If required, this data can be 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. VA is not responsible for Hard Drive Sanitization within GovCloud – action falls under FedRAMP ATO and is outside of the VA responsibilities.

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

Not applicable. e-VA only uses dummy data in the staging and testing environment

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.

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: Long-term storage of e-VA data increases the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, e-VA adheres to the VA Record Control Schedules (RCS) for each category or data it maintains. All electronic storage media used to store, process, or access e-VA records will be disposed of in adherence with Record Control Schedule 10-1 Section 4. (Disposition of Records). e-VA manages and retains data and information indefinitely in synchronization with the VBA Corporate Database. Data retained within the e-VA GovCloud environment will be synchronized in a near real-time manner with Corporate Database. Key data stored within e-VA includes VR&E participant identifiers, case notes, uploaded documentation, survey and participant supplied case activities. The breach or accidental release of e-VA data to inappropriate parties or the public will have Low impact on VA organizational operations, organizational assets, or individuals.

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***
VBA Corporate Database	Storage of active program participant data	• Name • Personal Phone Number • Personal Email Address	Secure HTTPS connection with SSL certificates

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: The risk might include end users who do not log out of the e-VA tool when away from their computers or mobile devices

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

Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 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***
e-VA application in vendor AWS GovCloud	Storage of active program participant data	• Name • Personal Phone Number • Personal Email Address	• SORN ID is Compensation, Pension, Education, and Vocational	Trusted Cloud Connection (TIC); Secure

			Rehabilitation and Employment Records—(58VA21/22/28) • MOU/ISA between the VA VR&E and TCI (prime contractor)	HTTPS connection

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 e-VA system does not share data outside of the VA. If there is data being shared outside of the department in the future, access controls will be implemented based on MOUs, contracts or agreements.

Mitigation: VA has contracted The Career Index (TCI) to deliver services that include maintaining VA data. A contract is in place that clearly articulates TCI's roles and responsibilities. Authorized TCI personnel access user level data to provision and provide the e-VA services. Access is controlled by authentication and is restricted to authorized individuals. TCI security policies address the required security controls that must be followed in order to protect PII.

Privacy Risk: e-VA does not currently have interconnections to any external information system. At such time as there becomes the need for a system interconnection, that status will change as approved by the PMO/ISSO.

Mitigation: The Interconnection Security Agreement (ISA) documentation is reviewed and updated annually

to confirm that all security requirements are still being met and that no changes to the connections have occurred. The annual review can be done as part of the annual internal security assessment and third- party assessment. The VA's prescribed risk intelligence platform is an integrated risk management solution (IRMS) and Security Operations, Analytics, and Reporting (SOAR) software that is used to assess an organization`s level of risk. Risk details updated within the IRMS and other security documents must also be reviewed to ensure they accurately reflect the status of each interconnection.

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.

VA Participants are informed of the e-VA services via US Mail letter from the VA VR&E Division (existing participants) or as part of the VA VR&E eligibility process (new participants). The information includes what the e-VA application is and what it does, how e-VA will communicate including the email address and cell phone number the application will be using as well as instructions on how to opt out. The first message from e- VA to any participant is always the opt-in/opt-out message. If the participants opts out, e-VA will not continue any further communications to the participant using the opted-out connection, unless the participants later specifically opts in.

A disclaimer warning will be displayed to all Vocational Rehabilitation Counselor (VRC's) and VR&E participants using e-VA directing them not to provide PII or PHI in open text comments or attachments. e- VA users must agree to the collection of data and information at every touchpoint and method where the data is collected.

It is estimated that the Notice to the Veteran that information will be collected is available via SORN ID Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— (58VA21/22/28) (link to be provided once uploaded to www.federalregister.gov) and in the Appendix A.

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

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

Yes, the VR&E participants may elect to not provide feedback through e-VA. There is no penalty or denial of service. This is a voluntary service.

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

e-VA is not used for collecting or storing any kind of health-related information. That said, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: There is a risk that Veterans may not know that the e-VA system exists within the Department of Veterans Affairs.

Mitigation: The e-VA cloud application will only be accessible to VR&E staff with the proper credentials and PIV card. Eligible program participant will be notified of the various new method of communication. At the initiation of the program for each participant, they will be required to read and accept the Terms of Service and Privacy Policy. Then they can "opt in" by selecting their preferred method of communication; email and/or text messages.

Mitigation: VA Participants are informed of the e-VA services via US Mail letter from the VA VR&E Division (existing participants) or as part of the VA VR&E eligibility process (new participants). The information includes what the e-VA application is and what it does, how e-VA will communicate including the email address and cell phone number the application will be using as well as instructions on how to opt out. The first message from e-VA to any participant is always the opt-in/opt-out message. If the participants opts out, e-VA will not continue any further communications to the participant using the opted-out connection, unless the participants later specifically opts in.

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.

e-VA is designed to be an information gathering system, not for information dissemination. There are no facilities for participants to view their own profile information or case status and related notes. However, all relevant information in e-VA is replicated to CWINRS and Veterans can request access to their records in CWINRS according to VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b). VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Authorized staff such as VRCs, have the ability to change participant data in their own case load. Likewise, authorized managers and administrators can correct participant data. If the participant discovers inaccurate or erroneous information, they can contact their VRC and request that the information be corrected. The CWINRS application (not the e-VA application) will be used to update and store corrected participant in the VBA Corporate Database upon immediate receipt of the request. Written notice of the change will be sent to the participant of the update within 5 working days.

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.

Correcting information will be covered as a topic during participant orientation. Business Rules will dictate the process for a VRC to notify a User with an Administrator role.

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.

Information in the e-VA application is not accessible to participants and the e-VA application will not have write access to update erroneously participant information in the Corporation Database If the participant discovers inaccurate or erroneous information, they can contact their VRC and request that the information be corrected. The inaccurate information will not be updated using this e-VA application. The legacy CWINRS application will be used by the VRC to update and store corrected participant in the Corporate Database. Written notice of the change will be sent to the participant of the update within 5 working days.

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:

Information in e-VA is not shared outside the VA and participants do not have direct access to information stored in e-VA.

Risk: There is a risk that incorrect participant information is in the VBA Corporate Database and the participant does not know how to access or correct it.

Mitigation: During the program eligibility process, participant email address and cell phone number will be verified and updated in the VBA Corporate Database. Updating of the participant's erroneous or changed email or cell phone number must be done by their VRC, who will use the legacy CWINRS to update and store corrected participant in the VBA Corporate Database.

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.

Role	Internal or External	Sensitivity Level (as determined by OPM guidance in FIN 10-06, Position Designation Requirements)	Authorized Privileges and Functions Performed
VA Workforce Members	Internal	Not Applicable	**Access AWS GovCloud – VA Application and/or Third-Party System services**
VA AWS GovCloud Administrators	**Internal**	**Privileged**	**Administer customer user accounts, modify Access AWS GovCloud – VA Application and/or Third-Party System configurations**

User roles identify the information and applications a user can access. To receive access to the e-VA system, another user of e-VA with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data per the table found above and described below.

All personnel authorized to access e-VA are considered privileged users, and are managed, identified, and authenticated in a consistent fashion in accordance with System Security Controls IA-2 and IA-2(1). Only Cloud Operations & Infrastructure and Security Operation users are authorized to perform day-to-day maintenance, operations, and monitoring of e-VA. In order to ensure only authorized personnel and communications can access administrative functions of the e-VA environment, the e-VA software relies on strong account and access management processes, in accordance with System Security Controls AC-2, separation of duties and least privilege enforcement in accordance with System Security Controls AC-5 and AC-6, strong logical authentication and access enforcement in accordance with System Security Controls AC-17 and IA-2, and networking and host-based protections in accordance with System Security Controls SC-7 and SI-4.

Special cases, such as OIG wanting to audit system logs, can be addressed by providing required users access through creation of "audit accounts" which can be setup via regular user account creation channels described in Section 8.2 below.

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.

eVA Systems Administrators:

The Career Index (TCI) is a contractor to the VA and maintain governing authority over all e-VA instances and cloud environments, where they maintain users' hierarchies, updates environments with system-level updates and new functionality, governs deployment activity and ensures user operability. The System Administrator is not a primary user of e-VA. All system administrators in TCI have signed an NDA with the VA during their on-boarding process.

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.

VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. Each site identifies personnel with significant information

system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The workforce will receive security awareness training annually as part of the Mandatory Training Program.

In addition, the training for the tool will include awareness training regarding the possible existence of PII/PHI information submitted from the Veterans, eligible dependents, and employees. Each employee is asked to refresh their understanding of the appropriate way to handle the data.

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

If Yes, provide:

1. *The Security Plan Status Pass*

2. *The Security Plan Status Date,12/28/21*
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.***

e-VA has been granted Authority to Operate (ATO) for three years, and is up for renewal on 01/21/2024. e-VA systems containing SPI are categorized as "MODERATE" under Federal Information Processing Standards Publication 199.

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.

The e-VA application and database are hosted as a Software-as-a-Service (SaaS) configuration in a vendor-owned (non-VA) Amazon Web Services (AWS) GovCloud environment, utilizing a Virtual Private Cloud (VPC). This application instance is only to the VA and thus is single-tenant. Each AWS VPC is completely segregated from other VPCs hosted on the AWS GovCloud with no way to move information or applications from VPC to VPC. The rest of the e-VA system components are VA custom-developed and are hosted in a VA Enterprise Cloud (VAEC), which resides in a VA-owned AWS GovCloud VPC. The vendor's AWS GovCloud VPC and the VAEC GovCloud VPC do not have overlapping boundaries.

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.

VA owns all PII/PHI related data, Contract #36C10E19P016

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.

Audit logs are maintained and have to be turned over if requested. Section 3.2.10 of MOU/ISA.

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 contract is with AWS and portions are hosted in AWS GovCloud and VAEC. Detailed roles and responsibilities are laid out in the MOU/ISA.

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 e-VA application will also communicate bi-directionally to its e-VA Windows Service module residing in the VAEC to perform the following two functions:

- **Storage of Participant Case Notes from the e-VA cloud application in the VBA Corporate Database:** The e-VA cloud application will send Case Note records for storage to the e-VA Windows Service module which resides in the VAEC. This connection will be over a Hypertext Transfer Protocol Secure (HTTPS) port 443 secure protocol. When the e-VA Windows Service receives these Case Note records, it will write them to the e-VA Interface Table (temporary data storage). These Case Notes records will be picked up by the IN PROCESS Java Service from the e-VA Interface Table, which will call a BGS web service to write the Case Note records to the VBA Corporate Database. Phase 2 of this project will use BIP web services instead of BGS web services.
- **Update Participant information from the VBA Corporate Database to the e-VA cloud application:** An OUT PROCESS Data Script will run nightly and will execute a query to the VBA Corporate Database to determine if there is any updated information on the active program participants (i.e., new participants in the program, new/updated participant email address, and new/updated participant cell phone numbers). This information will be written to an Output File, which will be sent to the e-VA VAEC VPC and stored on an SSH File Transfer Protocol (SFTP) server. The OUT PROCESS Shell Script will process the records in the output file and place them into the e-VA Interface Table. The records will then be picked up by the e-VA Windows Service module and sent to the e-VA cloud application's database for storage and used to communicate with the participants.

>>

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.

Chiquita Dixson 126558

Digitally signed by Chiquita Dixson 126558
Date: 2022.09.21 07:33:25 -04'00'

Privacy Officer, Chiquita Dixson

Brian R Kohler 290480

Digitally signed by Brian R Kohler 290480
Date: 2022.09.21 07:28:04 -04'00'

Information System Security Officer, Brian Kohler

LINDA RITCHIE

Digitally signed by LINDA RITCHIE
Date: 2022.09.14 07:28:57 -04'00'

Information System Owner, Linda Ritchie

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).

2021-24372.pdf (govinfo.gov)