Privacy Impact Assessment for the VA IT System called:

VA Enterprise Cloud (VAEC)

Enterprise Cloud Solutions Office (ECSO)

Veterans Health Administration

Date PIA submitted for review:

25 March 2022

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	(909) 583-6309
Information System Security Officer (ISSO)	Ron McKelvey	Ron.McKelvey@va.gov	304-596-8357
Information System Security Officer (ISSO)	Thomas Orler	Thomas.orler@va.gov	708-938-1247
Information System Owner	David Catanoso	David.catanoso@va.gov	732-440-9583

Abstract

The VAEC is the hosting environment for all OI&T cloud applications designed to ensure consistent utilization and execution of cloud application in alignment with the VA Cloud Strategy. VAEC provides Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud services, along with a set of common services, security, and connectivity between the cloud environments and the VA network. Numerous applications from across the VA Enterprise are hosted within the VAEC. The purpose of this PIA is to set up an Enterprise-Wide PIA that covers all the work, storage, platforms, etc. that are or will reside in the VAEC. This is an enterprise level hosting environment and platform for VA Applications which could include PII/PHI. Individual applications will submit and maintain their own PIA as applicable.

Overview

The VAEC is the hosting environment for all OI&T cloud applications designed to ensure consistent utilization and execution of cloud application in alignment with the VA Cloud Strategy. VAEC provides all levels of cloud services - IaaS, PaaS, SaaS along with a set of common services, security, and connectivity between the cloud environments and the VA network. VAEC hosts numerous applications from across the VA Enterprise. The purpose of this PIA is to set up an Enterprise-Wide PIA that covers all the work, storage, platforms, etc. that are or will reside in the VAEC. This is an enterprise level hosting environment and platform for VA Applications which could include PII/PHI. Individual applications submit and maintain their own PIA as applicable. The program office that owns the VAEC PIA is Enterprise Cloud Solutions Office (ECSO).

The cloud environments making up the VAEC, Microsoft Azure Government and Amazon Web Services GovCloud, are FISMA High rated. The tenants will have their own contracts with their specific vendor for ownership of data stored.

There is a low magnitude of harm for VAEC as it does not collect, process, or retain any PII/PHI/SPI. Tenants hosted within VAEC will vary and will specify their own magnitude of harm. VAEC itself is not privacy sensitive but the applications hosted could be and are therefore responsible for their own documentation specific to the applications.

The VAEC is part of the President’s IT Modernization 2017 initiative.

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 (VAEC GSS does not collect, but applications in the VAEC might)
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☒ Personal Phone Number(s) (if used for work)
☐ 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 Phone number
- Username
- The core VAEC systems only store username and phone number; the tenants hosted in the VAEC will require their own PIA as previously defined.
- VAEC General Support Services (GSS) will not process SSN however it is possible SSN could be included at some point by a tenant. The legal authority for SSN use or collection would be Executive Order 9397. Individual applications may collect data, but that transaction would be covered by the individual tenant's PIA.

PII Mapping of Components

The VAEC consists of seventeen key components that utilizes any PII (account information). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the VAEC and the reasons for the collection of the PII are in the table below.

The core Cloud systems will only store account information, the applications hosted on VAEC will require their own PIA as previously defined. SSN is not collected or stored by any core VAEC systems.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

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
IAM Active Directory (Azure)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
GitHub (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Ansible (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account,**

					logging of access
BigFix (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Centrify (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
EnCase (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
McAfee (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**

Nessus (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Splunk (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
ScienceLogic (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Dynatrace (Azure and AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Ansible Tower (AWS)	**Yes**	**Yes**	**Name, Username, Work Phone**	**Authentication**	**Encryption of data, controlled**

			(account information)		**access, logical isolation between each account, logging of access**
Workflow Manager (AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
VersionOne (AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
CloudKey (AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**
Turbot (AWS)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation**

					between each account, logging of access
AppDynamics (Azure)	**Yes**	**Yes**	**Name, Username, Work Phone (account information)**	**Authentication**	**Encryption of data, controlled access, logical isolation between each account, logging of access**

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.

Other than IAM and username data, the Core VAEC GSS systems will not collect and store PII. Applications hosted within VAEC may, but they will provide their own PIA documents to support.

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.

IAM, Direct SSOi integration with MS Active Directory. SSN is not collected by the VAEC. Applications hosted within VAEC will collect varying information which will be addressed in their individual PIAs.

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.

Active Directory integration has real-time synchronization in place. Applications hosted in VAEC would be covered under their own PIA.

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 VAEC is part of the President's IT Modernization 2017 initiative.
- Laws and Regulations: Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law, United States Code, and Homeland Security Presidential Directives.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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: LOW A user of the system shares his/her PIV card and Personal PIN with someone, and that person or persons access the VAEC without proper credentials and attempts to retrieve or destroy data.

Mitigation: Limit Access Based on log activity, appropriate responses can be executed immediately. User would have to be logged into VA Network first to access the VAEC.

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.

Name, username, and phone number are used for account information to access the VAEC and the GSS tools for official use only.

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

CloudWatch, Azure Monitoring, and Splunk audit logs are provided to the Computer Security Operation Center (CSOC) 24/7 alert team. The VAEC does not do any complex analytical tasks on individuals' data. The VAEC does not create or make available an unutilized information about individuals.

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?

Encryption of data at rest and data in transit (SSL, TLS). FIPS 140-2 compliant. Automated tools to validate and enforce data at rest controls continuously. Encryption keys and certificates are stored securely and rotated at appropriate times with strict access control.

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

Not applicable. Applications within the VAEC using PII/PHI would document this in their PIA.

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

Not applicable. Applications within the VAEC using PII/PHI would document this in their PIA. Name and phone number are "Rolodex information". All data at rest and data in transit is encrypted.

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

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

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

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

<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Only system level audit logging is stored on VAEC systems. Users access the VAEC via their VA Network Account. To get a VA Network Account, the user has gone through the VA onboarding process, which includes background check. Administrative access is granted via the VA's Non-eMail Enabled Account (NMEA - 0 account) request process. The VA requires manager approval on NMEA requests, processed through ePAS.

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

Access is granted to the VAEC via a user's VA Network account, which has name, username, and phone number stored in the VA's Active Directory. Data is retained only as long as a user has access. Applications hosted within the VAEC will have their own data retention documented in their PIA.

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.

Data is only retained while the user has an account in the VA's Active Directory. VAEC does not collect or maintain PII. Applications hosted within the VAEC will have their own data retention documented in their PIA.

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.

VAEC does not collect or maintain PII and a NARA approved retention schedule is not required. Applications hosted within the VAEC will have their own data retention documented in their PIA.

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

VAEC does not collect or maintain PII; there is no sensitive data for disposal. Applications hosted within the VAEC will have their own data retention and disposal documented in their PIA.

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

VAEC does not collect or maintain PII. Applications hosted within the VAEC will have their own data protection documented in their PIA.

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: Very Low There is a risk information could be stored for longer than necessary.

Mitigation: VAEC does not collected or maintain PII. Applications hosted within the VAEC will have their own data retention and disposal documented in their PI

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***
Active Directory	Authentication to VAEC	Receives Authentication Information	SSOi (Single Sign On)

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: Very Low There is a very low risk for information shared internally being shared internally.

Mitigation: VAEC does not collected or maintain PII. Applications hosted within the VAEC will have their own internal sharing documented in their PIA.

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***	***List the method of transmission and the measures in place to secure data***

			more than one)	
NA	NA	NA	NA	NA

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

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

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

Follow the format below:
<u>Privacy Risk:</u> Very Low A user must be on the VA network, authenticated with their PIV, to be able to access the VAEC. If a user is not supposed to have access to the VA network, but still does, the user could still access the VAEC if permissions to the security groups for access to the portal was not removed.

<u>Mitigation:</u> Even if a user got access to the VAEC when they weren't authorized, no PII is stored. Working with the CSOC and the Active Directory team, access would be removed.

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.

The VAEC does not collect any PII. No SORN is required. Name and phone information are collected by the VA during the onboarding process. Applications hosted within the VAEC will have their own notice information documented in their PIA.

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

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

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. If a user declines, they would not receive a PIV and would not have access to the VA network. Applications hosted within the VAEC will have their own notice information documented in their PIA.

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

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. If a user declines, they would not receive a PIV and would not have access to the VA network. Applications hosted within the VAEC will have their own notice information documented in their PIA.

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:

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: Very Low Although the VAEC does not collect PII, hosted applications might. If notice is not provided by the application, they would be unaware that their data is being collected.

Mitigation: Each application within the VAEC that collects PII will notify individuals with specific Notice of Privacy practices so that individuals are aware that their data is being collected.

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.

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. Active Directory information can be changed by the user by submitting a ticket to the Service Desk. Applications hosted within the VAEC will have their own user ability to ensure accuracy documented in their PIA.

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

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

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. Active Directory information can be changed by the user by submitting a ticket to the Service Desk. Applications hosted within the VAEC will have their own user ability to ensure accuracy documented in their PIA.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. Active Directory information can be changed by the user by submitting a ticket to the Service Desk. Applications hosted within the VAEC will have their own user ability to ensure accuracy documented in their PIA.

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.

The VAEC does not collect any PII. Name and phone information are collected by the VA during the onboarding process. Active Directory information can be changed by the user by submitting a ticket to the Service Desk. Applications hosted within the VAEC will have their formal redress documented in their PIA.

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: Very Low There is a risk that individuals will be unaware of how to correct any inaccurate information.

Mitigation: Users can correct AD information by submitting a ticket. All other information collected by the systems who use VAEC will be discussed in their individual PIAs.

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.

The same access policies that apply to the VA network apply to the VAEC. Access to the VAEC is requested via the ticketing system and approvals are received before a user's VA account is added to the appropriate security group(s) for access to the AWS or Azure portal or to the jump boxes.

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.

The same access policies that apply to the VA network apply to the VAEC. Contractors follow the VA onboarding process, which includes signing a confidentiality agreement. Access to the VAEC is requested via the ticketing system and approvals are received before a user's VA account is added to the appropriate security group(s) for access to the AWS or Azure portal or to the jump boxes. Contractors will see the user's name and phone number in the ticket.

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.

All users that access the VAEC have gone through the VA Onboarding process, which includes the required Privacy and HIPAA Training.

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.***

VAEC Microsoft Azure Government High Assessing, eMASS ID 87:

1. *The Security Plan Status*, APPROVED
2. *The Security Plan Status Date*, 21 March 2022
3. *The Authorization Status,* Authorization to Operate (ATO)
4. *The Authorization Date,*14 January 2021
5. *The Authorization Termination Date*, 14 January 2024
6. *The Risk Review Completion Date,* 21 March 2022, overall risk score Low
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).* HIGH

VAEC AWS GovCloud High Assessing, eMASS ID 86:

1. *The Security Plan Status*, APPROVED
2. *The Security Plan Status Date*, 21 March 2022
3. *The Authorization Status,* Authorization to Operate (ATO)
4. *The Authorization Date,*14 January 2021
5. *The Authorization Termination Date*, 14 January 2024
6. *The Risk Review Completion Date,* 21 March 2022, overall risk score Low
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).* HIGH

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.

VAEC uses the following FedRAMP Cloud Service Providers (CSPs): Amazon Web Services (AWS) GovCloud and Microsoft Azure Government. Both CSPs support Infrastructure as a Service, Platform as a Service, and 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.

The VA maintains ownership of the data, and selects which services can process, store, and host data. The CSP does not access or use the data for any purpose without agreement from the VA. VAEC determines where the data will be stored, including the type of storage and geographic region of that storage. VAEC manages access to its data, and access to services and resources through users, groups, permissions, and credentials that are internally controlled. VAEC chooses the secured state of the data. The CSP provides encryption features that protect data in transit and at rest and provides VAEC with the option to manage their encryption keys. *VAEC Enterprise Contract, NNG15SD22B VA118-17-F-2284*

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 CSPs automatically collect metrics, such as offering usage, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs. VAEC is the owner of its data (customer data). The CSP does not use customer data and has anonymized metrics to help them measure, support, and improve their services. The CSP has ownership of these anonymized metrics.

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.

Each application in the VAEC is responsible for their data. For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of their data and identities, on-premises resources, and the cloud components they control (which varies by service type). This is the Shared Responsibility Model for Security in the Cloud.

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).

Not applicable.

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.

JULIE C. DRAKE 969177 Digitally signed by JULIE C. DRAKE 969177
Date: 2022.04.13 14:33:35 -06'00'

Privacy Officer, Julie Drake

Albertino M. Estacio 119921 Digitally signed by Albertino M. Estacio 119921
Date: 2022.04.13 08:36:29 -07'00'

Information System Security Officer, Albert Estacio

Ronald J. McKelvey 179660 Digitally signed by Ronald J. McKelvey 179660
Date: 2022.04.13 09:03:53 -04'00'

Information System Security Officer, Ron McKelvey

Thomas J. Orler 178546 Digitally signed by Thomas J. Orler 178546
Date: 2022.04.13 12:01:20 -05'00'

Information System Security Officer, Thomas Orler

DAVID CATANOSO Digitally signed by DAVID CATANOSO
Date: 2022.04.13 01:05:28 -04'00'

Information System Owner, David Catanoso

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).