Privacy Impact Assessment for the VA IT System called:

VA Enterprise Architecture Management Suite (VEAMS)

Account Management Office (AMO) Office of Information and Technology (OIT)

Date PIA submitted for review:

October 5, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Alfred (Al) Sheets	Alfred.Sheets@va.gov	501-257-2111
Information System Owner	Stephen Gould	Stephen.gould3@va.gov	202-382-9332

Abstract

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

The VA Enterprise Architecture Management Suite (VEAMS) is a collection of web accessible capabilities assembled in an IT environment, which enables the creation, maintenance, and use of information generated for the VA Enterprise Architecture (EA) program. VEAMS was originally implemented in an on-premise solution but is now hosted in the VA Enterprise Cloud (VAEC) Microsoft Azure environment. VEAMS consists of EA content/modeling capabilities, the VA EA Repository (VEAR), and the VA Systems Inventory (VASI). It is a combination of COTS applications including Unicom System Architect / System Architect xTended Team (SA XT) and Microsoft Power BI business intelligence tools along with backend SQL Server Database. VEAMS provides a common point of entry but is organized using separate portals for accessing data. VEAMS capabilities are directly accessible by Governance Process participants, VA Enterprise Architects, VA EA Program Staff, and designated users across the VA enterprise.

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 IT system name and the name of the program office that owns the IT system are: a) VA Enterprise Architecture Management Suite (VEAMS) and b) Architecture & Engineering Service (AES), Account Management Office (AMO), Office of Information and Technology (OIT), Department of Veterans Affairs.

The business purpose of the program, IT system, or technology is to collect, develop, report, and maintain Enterprise Architecture (EA) data, artifacts, and work products for VA IT systems, solutions, initiatives, and modernization efforts. Its relation to the program office and agency mission is that VA EA information provides decision support guidance to VA senior managers for effective IT investment management focused on meeting the needs of Veterans.

The expected number of individuals whose information is stored in the system is ~2000 VA employees and associated contractors. A brief description of the typical clients or affected individuals includes VA IT system managers, IT investment decision makers, Enterprise Architects, Business Analysts, Portfolio Managers, VA Administration and Staff Office administrators, and their contractor support personnel.

The information in VEAMS consists of Enterprise Architecture-related models, databases, documents, artifacts, and work products; a detailed IT systems inventory; and associated websites and portals.

VEAMS comprises the following systems, applications, and tools:

- UNICOM System Architect (SA)—a COTS application that provides enterprise architecture analysis, design, and modeling support.
- UNICOM System Architect eXtended Team (SA XT)—a web interface to System Architect allowing users to make data operations via web browser rather than need the full desktop client software. SA XT also ships with an Operational Data Store and an API for direct interaction with the SA SQL database or ODS.

VEAMS collects a limited set of PII/III (see below) that is entered manually when an individual system record is created to identify key stakeholders associated with the system. The original source of the III is the VA GAL and this information is entered manually into VEAMS. Also, subsequent updates to the collected III can be made via a manual process where a monthly report of VA GAL changes is provided to VEAMS administrators who then review and manually make updates to this III as required.

VEAMS is operated and maintained in the VA Enterprise Cloud (VAEC) MS Azure Cloud environment which is FedRAMP authorized. A contract with Cloud Service Provider, Contractors and VA customers is in place that establishes who has ownership rights over data including PII.

It is unknown if the NIST 800-144 statement, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." is included in contracts with customers. The magnitude of harm if privacy related data is disclosed, intentionally or unintentionally is Minimal. There would be no impact to the reputation of CSP or its customers.

The current legal authority to operate (ATO) the IT system is the following eMASS security boundary: VA Enterprise Architecture Management Suite - 995. The current ATO for VEAMS is due to expire on 3/4/2022.

The completion of this PIA will not result in circumstances that require changes to business processes.

The completion of this PIA will not potentially result in technology changes.

VEAMS is not in the process of being modified. A review of existing System of Record Notices (SORNs) has identified the VA's Personal Identifiable Verification (PIV) system's SORN ID# 145VA005Q3 as the closest match found. The SORN can be viewed and accessed by clicking on the following link: http://www.rms.oit.va.gov/sor_records.asp.

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.

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
☐ Other Unique Identifying Information (list below)

- Personal Phone Number (checked above): Phone number from the GAL where the GAL entry includes a personal phone number that is used as a business number.

- VEAMS is a repository and authoritative source of IT enterprise architecture information for all of VA including EA artifacts, models, work products, visualizations, system inventories, web sites, and other data collected to provide VA stakeholders and senior management with key, decision-making information for proper allocation of IT investments. At this time, the only Sensitive Personal Information (SPI) collected in VEAMS is Individually Identifiable Information (III) limited to employee names, work organizations, work title, work emails addresses, and work phone numbers as documented in the VA Global Address List (GAL) and that are assigned to system and other records. While all emails and phone numbers in the VA GAL should be provided and managed by VA, there are instances, such as with contractor personnel, where personal or contractor-specific contact information could be listed.

PII Mapping of Components

VA Enterprise Architecture Management Suite (VEAMS) consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VEAMS and the functions that collect it are mapped 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.

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
VA Enterprise Repository (VEAR) (UNICOM System Architect (SA))	**Yes**	**Yes**	**Employee/contractor name** **Work phone number** **Work email**	**VASI component collects ID information of system stakeholders**	**Only uses data already available in the VA GAL and only describes official duty contact information**

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 source of key stakeholder III in VEAMS is the VA Global Address List (GAL), which is the authoritative source of VA employee and contractor identification data.

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.

Key stakeholder PII is collected in VEAMS/VASI manually by EA support staff. An automated process is leveraged to identify any stakeholders that have been removed from the GAL so those stakeholders can be manually removed from VASI.

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.

The information is validated by IT System stakeholders (VASI Information Owner) to confirm the correct individual is associated with a particular system. The VASI Technical Work Group (VTWG) oversees this process and approves significant changes to the repository.

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 information is required to meet the requirements of the Department of Homeland Security Presidential Directives 12 (HSPD-12) and Federal Information Processing Standard (FIPS 201). The information is protected by the Privacy Act, 5 USC Section, 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901-905 in VA system of records "Police and Security Records-VA (103VA07B)." (Source: PIV SORN ID# 145VA005Q3).

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:

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

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

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

<u>*Principle of Data Quality and Integrity:*</u> *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:
<u>Privacy Risk:</u> Minimal - if the data were accessed by unauthorized individual or otherwise breached, professional or financial harm will not result for the individual affected.

- Per the Principal of Purpose Specification, the restricted set of Key Stakeholder information collected in VASI is critical for the proper collection and upkeep of the IT System Information used to manage VA IT Systems and Investments.
- Per the Principal of Minimization, the Key Stakeholder information is restricted to only those data elements necessary to identify and locate the person assigned responsibility for a specific VA IT system.

<u>Mitigation:</u> VEAMS employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. Many of the security controls are common security controls throughout the VA. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our security controls follow VA 6500 Handbook and NIST SP800-53 Moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of the facility's common security controls.

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.

VEAMS is an internal VA resource for collecting, maintaining, and distributing VA Enterprise Architecture information such as enterprise and segment architecture models and an inventory of

IT systems for use by VA managers and other internal stakeholders to make effective investment decisions in support of VA's principal responsibility to care for the Veteran and their families.

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

- Microsoft SQL Server Relational Database – core database management tool used to define the VEAMS data environment, create and maintain the repository, and host the systems inventory
- Unicom System Architect (SA) – Enterprise Architecture modeling and management tool which includes a browser-based, user-driven data management and business transformation platform that VEAMS uses to provide users access to the VEAMS repository, systems inventory, and EA artifacts.
- SharePoint - manages documents and information as well as creates workflow processes to interact with, tracks, and reports/audits information.
- WordPress – website management tool

None of these system components is used to manipulate, derive, transform, or create new sensitive information associated with the limited III captured in VEAMS — a restricted set (5 data elements) of identifying information about key stakeholders who manage and maintain systems listed in VASI which are sourced from the VA GAL.

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?

- While in transit, these systems connect via HTTPS encryption.
- JSON API calls also connect via HTTPS encryption.
- Email communications regarding system information, user accounts are encrypted.

- Any communication regarding user and system information without encryption, such as IP addresses and server names (although allowed among team members) will be flagged by Security.
- The organization is using Single Sign-on and PIV card for logging into the system.
- While at rest, the system is being scanned for any discrepancy, and notified security for review.
- Backup data is in secured Azure VM.
- Only approved elevated privilege user with Token USB, in proper group role, have access to the Azure VM servers.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? **Not Applicable**

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.

The users of VEAMS are restricted to VA employees and authorized contract staff located within VA's security firewalls. This same set of users already has unrestricted access to all PII stored in the VA GAL and accessible via VA's Outlook email system. Therefore, there is no access restriction for the III used by VEAMS because its source is the VA GAL.

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

VEAMS retains the following Individually Identifiable Information:

a. Name
b. Work Title
c. Organization
d. Work Email Address
e. Work Phone Number (except where the VA employee/contractor has provided a personal phone number for use in the GAL)

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.

VEAMS records are retained in accordance with records retention standards approved by the Archivist of the United States, the National Archives and Records Administration, and published in Agency Records Control Schedules. A minimum of three years or as documented in the NARA retention periods, HIPAA legislation (VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).

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.

The PIV records are retained in accordance with the General Records Schedule 1 and the Office of Personal Management Recordkeeping Manual as approved by NARA.

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

PIA's are part of the FISMA report and looked at by OMB and upper VACO Officials. When the VEAMS system owner decides the data is no longer needed, records are destroyed by shredding, burning, or by erasing the magnetic media. Automated storage media is retained and disposed of in accordance with deposition authorization approved by the Archivist of the United States. The authorized destruction of records that are classified or otherwise restricted from disclosure by statute, such as PA or Title 38 U.S.C., must be witnessed by a Federal employee or a contractor employee. If a contract is used to dispose of restricted VA records, the facility Records Officer must authorize the use of a contractor or subcontractor employee to witness the destruction.

In VA the destruction of national security information, including the method of destruction, must be approved by the VA Security Officer, Office of the Assistant Secretary for Security and Law Enforcement. Any contract for sale of VA records must prohibit their resale for use as records or documents. VEAMS records are destroyed at VA owned facilities.

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

Since the III used in VEAMS is the same available to all VA employees and contract staff via the VA GAL and VA Outlook email system there are no specific techniques used by VEAMS to minimize the risk to privacy of using PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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: Minimal – the risk of maintaining the III data in VEAM is not affected by the duration of the time it is retained. If, at any time, the data were accessed by unauthorized individual or otherwise breached, professional or financial harm will not result for the individual affected.

Mitigation: VEAMS retains only the information necessary for its purpose and the III is retained for only as long as it is accurate. Additionally, VEAMS adheres to the VA RCS schedules for each category or data it maintains. When the retention date is reached for a record, VEAMS will carefully disposes of data by the determined method.

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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Corporate Data Warehouse (CDW)	Provide system stakeholder/POC data per request from CDW	• Name • Work Phone Number ○ Source: VA Global Address List (GAL) ○ Some GAL records contain personal phone number where user opts to use personal phone number for work purposes.	JSON API using HTTPS

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

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

Follow the format below:
Privacy Risk: Minimal - Since the III used in VEAMS is the same available to all VA employees and contract staff via the VA GAL and VA Outlook email system, the risk to privacy of using such PII is equal to that of any VA user with access to email.

Mitigation: A privacy policy statement is available and directly accessible to all VEAMS users via its web-enabled user interface.

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 3.11 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 shared/received 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***
Not Applicable				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Not applicable

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: Not applicable

Mitigation: Not applicable

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Yes - VEAMS is a web-enabled system and provides a privacy policy notice to all users. The notice is accessible from VEAMS repository homepage located at: https://vaww.ea.oit.va.gov/vear. The Privacy Policy link is listed at the bottom of the homepage.

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

Personnel who are assigned as key stakeholders in VEAMS can correct inaccurate or erroneous information or decline to provide this information via the following methods:

a. Stakeholders can update their III in the VA GAL via established update procedures. When changes are implemented in the VA GAL, a monthly report is provided to VEAMS administrators who then manual make changes to VEAMS as required.
b. Stakeholders can reach the VEAMS helpdesk by email at VASITeam@va.gov to notify a system administrator about any required change.

In the case where an individual declines to provide the III information used in VEAMS, there is no inherent denial of service for access to VEAMS.

Additional notice is provided through this PIA, which is available online as required by the eGovernment Act of 2002, Public Law 107-347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA SORN (SORN ID# 145VA005Q3) which is published in the Federal Register and available online.

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

Since the III used by VEAMS is provided by the VA GAL, any rights to consent to particular uses of the information are determined by the VA GAL system and are not the responsibility of VEAMS.

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:
<u>Privacy Risk:</u> There is no risk associated with notice relative to VEAMS PII information.

<u>Mitigation:</u> A privacy policy statement is available and directly accessible to all VEAMS users via its web-enabled user interface.

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.

All VA employees and contractor staff may obtain access to VEAMS. Procedures and links for accessing VEAMS and its components are available via the VA EA intranet website accessible using the following URL: https://vaww.ea.oit.va.gov/veams-capability-access-request/.

In addition, specific questions about individual information in VASI can be directed to: VASITeam@va.gov.

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.

Personnel who are assigned as key stakeholders in VEAMS can correct inaccurate or erroneous information or decline to provide this information via the following methods:

- Stakeholders can update their III in the VA GAL via established update procedures. When changes are implemented in the VA GAL, a monthly report is provided to VEAMS administrators who then manual make changes to VEAMS as required.

- Stakeholders can reach the VEAMS helpdesk by email at VASITeam@va.gov to notify a system administrator about any required change.

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.

Training materials and resources for VEAMS include directions to contact the VEAMS Helpdesk by email at VASITeam@va.gov whenever they need to correct any information including the PII.

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.

VEAMS users do have the ability to update or otherwise redress their PII in VEAMS via the methods outlined in Section 7.2 above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:
Privacy Risk: There are no risks to access, redress, or correction of PII in VEAMS because users have the ability to update their PII via the methods outlined in Section 7.2 above.

Mitigation: No additional VEAMS-specific mitigation is required.

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.

All VA employees and contractor staff may obtain access to VEAMS. Procedures and links for accessing VEAMS and its components are available via the VA EA intranet website accessible using the following URL: https://vaww.ea.oit.va.gov/.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor

confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

- Contractors have access to VEAMS and its PII on a daily basis. The entire VEAMS solution is maintained and updated by contractors under the direction of VA Government Managers.
- Contracts are reviewed at least annually by the CO, COR, and contractor management.
- Contractors are critical to proper operation, maintenance, and development of VEAMS on a daily basis.
- The clearance requirement for the VEAMS solution environment is National Agency Check with Inquiries (NACI) Public Trust and all contractors must meet this requirement before obtaining access to VEAMS.
- Yes, contractor confidentiality and non-disclosure agreements (NDAs) are required and are on file.

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 VA Employees and contractors are required to complete and submit certification for annual privacy and security training the VA Training Management System (TMS). No additional privacy and security training is required for VEAMS.

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.***

1. Approved/signed
2. 1/11/2021
3. Authorization to Operate (ATO)
4. 3/4/2021
5. 3/4/2022
6. 9/23/2020
7. LOW

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology?

If so, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

VEAMS is hosted at VAEC Azure and inherits security controls from VAEC Microsoft Azure Government High Assessing.

9.2 Identify the cloud model being utilized.

Example: 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.

Platform as a Service (PaaS)

9.3 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.

VEAMS is hosted in VAEC Microsoft Azure Government and uses the same contract as all VA systems being hosted on this platform.

9.4 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.

Not applicable

9.5 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.

VEAMS is hosted in VAEC Microsoft Azure Government and uses the same contract as all VA systems being hosted on this platform.

9.6 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 9. 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 Privacy Officers

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

RITA K GREWAL 114938 Digitally signed by RITA K GREWAL 114938
Date: 2021.10.28 19:10:18 -04'00'

Privacy Officer, Rita Grewal

Alfred D. Sheets 3441543 Digitally signed by Alfred D. Sheets 3441543
Date: 2021.11.02 13:32:57 -05'00'

Information System Security Officer, Alfred (Al) Sheets

Stephen L. Gould 927251 Digitally signed by Stephen L. Gould 927251
Date: 2021.10.13 13:28:23 -04'00'

Information System Owner, Stephen Gould

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).