Privacy Impact Assessment for the VA IT System called:

Veterans Experience Integration Solution (VEIS)

Veterans Affairs Central Offices (VACO)

Enterprise Program Management Office (EPMO)

eMASS ID #2314

Date PIA submitted for review:

2/4/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov OITPrivacy@va.gov	202-632-8423
Information System Security Officer (ISSO)	Albert Estacio	albert.estacio@va.gov	909-528-4958
Information System Owner	Curtis Brown	curtis.brown6@va.gov	737-298-5688

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

Veterans Experience Integration Solution (VEIS) provides integration services to VA backend data providers for Dynamic365 applications utilizing custom-developed middleware platform services.

Overview

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

1 *General Description*

A. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
Veterans Experience Integration Solution (VEIS) is an integration framework, implemented as a PaaS, with 250+ application programming interfaces (APIs) that supports application connections to VA Enterprise Systems to retrieve authoritative Veteran data. Built on a microservices architecture, VEIS utilizes Dynamics365 Plug-ins, Azure API Services, and Azure API Management (APIM) Services that provide the patterns and structure for Dynamics365 LOB applications to VA Enterprise Systems for information and data processing. The data is consumed by VA Dynamics 365 applications such as COMM Care, and Unified Desktop Optimization (UDO). VEIS hosts an ATC (Authority to Connect) for the following applications BTSSS, TMP (including VA Mil), UDO, COMMCare and PATS-R.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

Veterans Experience Integration Solution (VEIS) is VA owned and operated by Enterprise Program Management Office (EPMO).

2. *Information Collection and Sharing*

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

Approximately, one million (1,000,000) beneficiaries.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

D. *What is a general description of the information in the IT system and the purpose for collecting this information?*

Veterans Experience Integration Solution (VEIS) collects and processes PII/PHI and network security records to assist in processing care for Veterans and Beneficiaries as well as monitor the VA Network.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

F. Are the modules/subsystems only applicable if information is shared?

Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

G. *Is the system operated in more than one site to include primary and secondary 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?*

Secondary site is not required for business reporting services. Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 1151 1705, 1710, 1712, 1717, 1720, 1721, 1727, 1741–1743, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014. Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1787, 1802, 1812, 1813, 1821, Public Law 111–163 section 101. 38 U.S.C. 1705, 1710, 1722, 1722(a), and 5 U.S.C. 552(a). Title 38, United States Code, Chapter 73, section 7301(b). Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 5 U.S.C. 5514. 38 U.S.C. 513. 38 U.S.C. 7304. Title 38, United States Code, Sections 304.

I. What is the SORN?

23VA10NB3, Non-VA Care (Fee) Records-VA (7/30/2015);
2015-18646.pdf

54VA10NB3, Veterans and Beneficiaries Purchased Care
Community Health Care Claims, Correspondence, Eligibility,
Inquiry and Payment Files-VA (3/3/2015);
2015-04312.pdf

121VA10, National Patient Databases-VA (4/12/2023):
2023-07638.pdf

155VA10/88 FR 63678, Customer Relationship Management System (CRMS)-VA (9/15/2023) https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf

57VA10/88 FR 4882, Voluntary Service Records-VA (1/25/2023)
https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-01437.pdf

100VA10H / 86 FR 6988; “Patient Advocate Tracking System Replacement (PATS-R)—VA” (1/25/2021) https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01501.pdf
Authority for maintenance of the system: Title 38, United States Code, Chapter 73, section 7301(b).

58VA21/22/28/86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

57VA10 / 88 FR 4882, Voluntary Service Records-VA (1/25/2023)
https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-01437.pdf

150VA10/88 FR 75387, Enterprise Identity and Demographics Records-VA (11/2/2023) https://department.va.gov/privacy/system-of-records-notices/

79VA10/85 FR 84114, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (12/23/2020) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

24VA10A7/85 FR 62406 – Patient Medical Records - VA (10/2/2020) https://www.oprm.va.gov/privacy/systems_of_records.aspx

168VA005/86 FR 6975, Health Information Exchange-VA (01/25/2021) https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The system of record notices does not require amendment.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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. It must also match the information provided in question 3.4 of the PTA.

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
☒ **Full** Social Security Number
☒ **Partial** Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account Numbers
☒ Certificate/License Numbers[1]
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender/Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☐ Date of Death
☐ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements: Marital Status, Preferred Language, Preferred Name, Religion, Record identification VA Profile ID, Active Prescription Status, Military Connection, Time served, Matching patient Veteran, Sensitivity levels, Demographics, Release from Active-Duty Date, Username,
Veteran and Beneficiary: Veteran, Insurance information, claim information, referral information, relationship to veteran or beneficiary, determination, eligibility status, enrollment status, claim status, corresponding ID, payments, call notes, Veteran Benefits payments

Members of the Public/Individuals: office address, relationship to "customer", Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data, Health Data Repository (HDR) data.

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

Note: Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

1.2 List the sources of the information in the system

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information is not generated in VEIS, the information comes from the Veteran or sources of the information is collected for the minor applications listed in this PIA. (See section 4.1b for list of applications).

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

Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Veterans Experience Integration Solution (VEIS): The VEIS does not provide any reports and does not provide any analytics with PII/PHI information. Application projects (VA Dynamics 365) own the business reports utilizing data from resources hosted in VEIS.

1.3 Methods of information collection

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

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

Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

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

The information is not collected on a form. Veterans Experience Integration Solution (VEIS): Azure Platform as a Service (PaaS) integration solution for applications to interface with back-end VA data.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

Veterans Experience Integration Solution (VEIS): Data is transmitted from/stored for the minor applications and not checked for accuracy.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

Veterans Experience Integration Solution (VEIS): No commercial aggregator is used.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 1151 1705, 1710, 1712, 1717, 1720, 1721, 1727, 1741–1743, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014. Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1787, 1802, 1812, 1813, 1821, Public Law 111–163 section 101. 38 U.S.C. 1705, 1710, 1722, 1722(a), and 5 U.S.C. 552(a). Title 38, United States Code, Chapter 73, section 7301(b). Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 5 U.S.C. 5514. 38 U.S.C. 513. 38 U.S.C. 7304. Title 38, United States Code, Sections 304.

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> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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: The applications collect Personally Identifiable Information (PII), and if this information were released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to those individuals.

Mitigation: Application mitigates the risk of identity theft by requiring all applicable Contractors and VA employees who engage with VEIS to complete all the following data security and privacy VA trainings: VA Privacy and Information Security Awareness and Rules of Behavior Training, and Privacy and HIPAA focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

Section 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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Fax, Number, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers,	File Identification purposes	Not used

Medications, Medical Records, Race/Ethnicity, Tax Identification, Gender, Mother’s Maiden Name, Integrated Control Number (ICN), Military History/Service Connection, Next of kin, Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments, Demographics, Contact History, Electronic Data Interchange Personal (EDIPI), Exam Appointment Information, Updates of contact history, Data File Numbers (DFN), Release from Active-Duty Date, Username, Veteran and Beneficiary: claim information, referral information, relationship to veteran or beneficiary, sensitivity, determination, eligibility status, enrollment status, claim status, corresponding ID, Members of the Public/Individuals: office address, relationship to “customer”, Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data, Health Data Repository (HDR) data		

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Veterans Experience Integration Solution (VEIS). VEIS does not use analytical tools to evaluate PII/PHI. Application projects (VA Dynamics 365) own the business artifacts utilizing resources hosted in VEIS.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Veterans Experience Integration Solution (VEIS) does not create any new information.

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data within the VA network is FIPS 2.0 encrypted and at rest, disk is encrypted.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

VEIS uses HTTPS, TLS, oAuth tokens and OSP APIM for additional encryption.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. HTTPS using SSL encryption is used between internal VA systems. Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. VEIS uses HTTPS, TLS, oAuth tokens and OSP APIM for additional encryption.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

Principle of Transparency: *Is the PIA and SORN, if applicable, clear about the uses of the information?*

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

2.4a How is access to the PII determined?

VEIS has an onboarding standard operating procedure that controls access to PII.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Criteria, procedures, controls, and responsibilities regarding access are documented in the VEIS SOP located and stored on the associated Veterans Affairs VEIS Confluence page.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates. (including but not limited to: VA 6500, Trusted Internet Connection (TIC), Privacy Impact Analysis (PIA) / Privacy Threshold Analysis (PTA), System of Record Notice (SORN), and the application's Authority to Operate (ATO).

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

It is the responsibility of the project making the request and VEIS to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates (including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

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

Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Fax, Number, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Tax Identification, Gender, Mother's Maiden Name, Integrated Control Number (ICN), Military History/Service Connection, Next of kin, Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments, Demographics, Contact History, Electronic Data Interchange Personal (EDIPI), Exam Appointment Information, Updates of contact history, Data File Numbers (DFN), Release from Active-Duty Date, Username, Veteran and Beneficiary: claim information, referral information, relationship to veteran or beneficiary, sensitivity, determination, eligibility status, enrollment status, claim status, corresponding ID, Members of the Public/Individuals: office address, relationship to "customer", Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data, Health Data Repository (HDR) data

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

Application projects (VA Dynamics 365) own the business artifacts /data from resources hosted in VEIS. Retention details are determined by Application teams. Depending on the type of information being retained, the timeframe could range anywhere from 9 months to 75 years. Information is retained according to the disposition instructions documented in Records Control Schedule: VHA RCS 10-1 10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf .

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Application projects (VA Dynamics 365) own the business artifacts /data from resources hosted in VEIS. Retention details are determined by Application teams.

3.3b Please indicate each records retention schedule, series, and disposition authority?

Record Control Schedule (RCS) 10–1 item XXXVIII
Records Control Schedule (RCS) 10–1, 1925.1, GRS 6.5, item 020 DAA-GRS 2017-0002- 0001
RCS 10–1, Item Number 3020.10–3020.11.
GRS 2.1, item 100 DAA-GRS 2014-0002-0014
GRS 2.1, item 101 GRS 2.1, item 102 DAA-GRS 2014-0002-0015
GRS 2.1, item 110 DAA-GRS 2014-0002-0018
GRS 2.1, item 111 DAA-GRS 2014-0002-0019
1300.1 (N1–15–05–2, Item 1-6)
GRS 4.3 Items 020, 030, 031
Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100
(RCS) 10–1, Item 2000.2. DAA-GRS 2013-0005-0004, item 020
(RCS 10–1) 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)
GRS 4.3 Items 020, 030, 031

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

https://www.va.gov/vapubs/search_action.cfm?dType=1.

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

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

No data is used 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

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

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

Principle of Minimization: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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: There is a risk that the information maintained by VEIS may be retained for longer than necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risks of information retention, VEIS will adhere to NARA Records Control Schedule. When a records retention date is reached, the individuals' information is disposed of by the method described in RCS 10. Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a VEIS consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VEIS and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
UDO, CommCare, PATSR	No	Yes	Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Fax, Number, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Tax Identification, Gender, Mother's Maiden Name, Integrated Control Number (ICN), Military History/Service Connection, Next of kin, Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments, Demographics, Contact History, Electronic Data Interchange Personal (EDIPI), Exam Appointment	File Identification purposes	This application is within VA and has FIPS 2.0 encryption.

			Information, Updates of contact history, Data File Numbers (DFN), Release from Active-Duty Date, Username, Veteran and Beneficiary: claim information, referral information, relationship to veteran or beneficiary, sensitivity, determination, eligibility status, enrollment status, claim status, corresponding ID, Members of the Public/Individuals: office address, relationship to “customer”, Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data, Health Data Repository (HDR) data		
CLEAR_CRM, HECImaging_CRM, HECWRap_CR	No	Yes	Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Fax, Number, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical	File identification purposes	This application is within VA and has FIPS 2.0 encryption.

			Records, Race/Ethnicity, Tax Identification, Gender, Mother’s Maiden Name, Integrated Control Number (ICN), Military History/Service Connection, Next of kin, Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments, Demographics, Contact History, Electronic Data Interchange Personal (EDIPI), Exam Appointment Information, Updates of contact history, Data File Numbers (DFN), Release from Active-Duty Date, Username, Veteran and Beneficiary: claim information, referral information, relationship to veteran or beneficiary, sensitivity, determination, eligibility status, enrollment status, claim status, corresponding ID, Members of the Public/Individuals: office address, relationship to		

			“customer”, Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data, Health Data		
TMP	No	Yes	Scheduled appointment Information, Patient ICN, Patient Contact Information, Patient Identification Information, Name, DOB	File Identification purposes	This application is within VA and has FIPS 2.0 encryption.
FCMT_MSCRM,	No	Yes	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Previous Medical Records, EDIPI	File Identification purposes	This application is within VA and has FIPS 2.0 encryption.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Customer Relationship Management Unified Desktop Optimization (CRM UD-O	Identification	Name: First Name, Last Name, (MVI will return interface Change Notice ICN and Data File Numbers (DFN) for the matching record) Social Security Number, Date of Birth, EDIPI, Mailing Address, Zip Code, Phone Number(s), Email Address, Exam Appointment Information, Veteran sensitivity levels, payment details, demographics, updates contact history, Veteran relationships (spouse and next of kin), Veteran insurance information, Veteran contact history notes, Veteran ratings, Veteran awards, and payments, Veteran Benefits payments	HTTPS using SSL encryption and Certificate exchange with the VEIS App services hosted on Microsoft Azure Government cloud (MAG)
Community Care (CommCare)	Identification	Name, social security number (SSN), date of birth, mother's maiden name, mailing address, phone number, fax number, email address, emergency contact information, financial information, health insurance beneficiary numbers account numbers, taxpayer identification number, claim information, referral information, relationship to veteran or beneficiary,	HTTPS using SSL encryption and Certificate exchange with the VEIS App services hosted on Microsoft Azure Government cloud (MAG)

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		Department of Defense (DoD) Electronic data interchange personal identifier (EDIPI), sensitivity, determination, eligibility Status, enrollment Status, claim status, ICN, corresponding ID	
Patient Advocate Tracking System – Referral (PATS-R)	Identification	Name, Social Security Number (SSN), Date of Birth (DOB), Phone Number(s), Fax Number, Department of Defense (DoD) Electronic Data Interchange Personal Identifier (EDIPI), Ethnicity, Race, Marital Status, Preferred Language, Religion, Sexual Orientation, Pronoun, Self-Identified Gender Identity (SIGI), Preferred Name	HTTPS using SSL encryption and Certificate exchange with the VEIS App services hosted on Microsoft Azure Government cloud (MAG)
Member Services (MS-CRM)	Identification	Name, DOB	HTTPS using SSL encryption and Certificate exchange with the VEIS App services hosted on Microsoft Azure Government cloud (MAG)
Telehealth Management Platform (TMP)	Identification	Scheduled appointment Information, Patient ICN, Patient Contact Information, Patient Identification Information, Name, DOB	HTTPS using SSL encryption and Certificate exchange with the VEIS App services hosted on Microsoft Azure Government cloud (MAG)
Federal Case Management Tool (FCMT)	Identification	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact	HTTPS using SSL encryption and Certificate exchange with the VEIS App

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		Information (Name, Phone Number, etc. of a different individual), Previous Medical Records, EDIPI	services hosted on Microsoft Azure Government cloud (MAG)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Privacy information may be inadvertently released to unauthorized individuals.

Mitigation: VEIS will adhere to information security requirements instituted by the VA OIT. Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

Information is not shared with external organizations.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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.

Information is not shared with external organizations.

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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: VEIS does no external sharing or disclosure.

Mitigation: VEIS does no external sharing or disclosure.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Application projects (VA Dynamics 365) own the data and are expected to provide the notification.

6.1b If notice was not provided, explain why.

Application projects (VA Dynamics 365) own the data and are expected to provide the notification.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Application projects (VA Dynamics 365) own the data and are expected to provide the notification.

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 opportunity and right to decline to provide information and any penalty or denial of service is determined by each application project.

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 right to consent to uses of the information and how to exercise that right is determined by each application project.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: VEIS users do not adhere to information security requirements instituted by the VA OIT, if PII is disclosed, the trust and reputation in VA and the call centers could be harmed consequently.

Mitigation: Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. Multi factor authentication, encryption,

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 The procedures that allow individuals to gain access to their information.

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

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

The VHA Notice of Privacy Practices explains the rights of the Veteran to request access to their records. AVA Form 10-5345a (Individual's Request for a Copy of Their Own Health Information) may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by, the System Manager for the concerned VHA system of record, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access will be granted.

VHA Notice of Privacy Practices is located here. (Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946)

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

VEIS is not exempt from the access provisions of the Privacy Act.

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

The system is a Privacy Act system.

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.

Application projects (VA Dynamics 365) own the data and are expected to correct inaccurate or erroneous information.

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.

Application projects (VA Dynamics 365) own the data and are expected to correct inaccurate or erroneous information.

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

Application projects (VA Dynamics 365) own the data and are expected to provide alternatives to the individual if no formal redress is provided.

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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

<u>Mitigation:</u> The application that is responsible for the data mitigates the risk of incorrect information in an individual's records by informing Veterans of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. Additionally, access, redress, and correction policies and procedures are outlined in the applicable SORNS.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

To gain access and modify resources in the VEIS Platform, the VA requires users to submit a request for Elevated Privileges through the ePAS portal. The ISO is the Account Manager who approves/disapproves requests.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Other agencies or external agency users do not have access to the VEIS platform.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

The list of roles represents a standard set of roles deemed appropriate for the CRM application teams to perform their job duties for their VEIS-hosted components. Additional permissions may be requested if justified/needed, but these would require written approval from the VEIS team **before** submitting the ePAS. To inquire about additional permissions that deviate from common roles, a "Access Request" ticket must be submitted through the VEIS Platform Intake Portal. All roles fall under these standard set of roles: CyberArk – CyberArk User – Production; Group – VA\VA PAS Users; VA-Azure roles. As the platform administrators, VEIS team members are authorized to request access to all available roles to properly support application teams.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

There is a BAA but there is no standalone NDA. Through the Contractor Rules of Behavior, VEIS personnel agree not to share sensitive information. VEIS adheres to information security requirements instituted by the VA OIT. Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

8.2a. Will VA contractors have access to the system and the PII?

Yes.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors have administrative responsibilities.

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.

VEIS adheres to information security requirements instituted by the VA OIT. Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 12/16/2024*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date:* 05/27/2024
5. *The Authorization Termination Date: 05/27/2025*
6. *The Risk Review Completion Date:* 05/24/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

VEIS is middleware running in the VA-authorized and controlled Cloud Computing Environment, Veterans Affairs Enterprise Cloud (VAEC) Microsoft Azure Government (MAG). The system and data will reside in the VAEC MAG environment. VA Enterprise Cloud's Azure platform and associated services leveraged are categorized FedRAMP High. VEIS aligns with the Platform as a Service (PaaS) model.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). *(Refer to question 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO. The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure. Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO. The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO.

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.

No ancillary data is collected by this system.

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.

Microsoft is responsible for Azure and maintains, validates, and monitors all security efforts inside of Azure.

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).

VEIS does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.02.12 14:44:55 -05'00'

Privacy Officer, Tonya Facemire

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2025.02.19 06:31:23 -08'00'

Information Systems Security Officer, Albert Estacio

CURTIS BROWN

Digitally signed by CURTIS BROWN
Date: 2025.02.12 14:51:08 -06'00'

Information Systems Owner, Curtis Brown

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)