Privacy Impact Assessment for the VA IT System called:

Veterans Information Solution Cloud

VACO

Veteran Experience Office (VEO)

eMASS ID #2208

Date PIA submitted for review:

September 12, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Anmar Faik	Anmar.Faik@va.gov	202-459-8385
Information System Security Officer (ISSO)	Eric Abraham	Eric.Abraham@va.gov	512-326-7422
Information System Owner	Alexander Torres	Alexander.Torres@va.gov	703-300-5511

Abstract

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

Veterans Information Solution (Cloud) (VIS-AWS) is an intranet web-based application that provides a consolidated view of comprehensive eligibility utilization data from across the Veterans Benefit Administration (VBA). VIS-AWS provides access to profile, service, rating and award information and benefits payments data that is replicated from the Department of Defense (DoD) to Department of Veterans Affairs (VA)/Department of Defense Identity Repository (VADIR) database. VIS-AWS also displays data from the VBA corporate database.

VIS-AWS provides a consolidated view of comprehensive eligibility and benefits utilization data from the Department of Defense (DoD). VIS-AWS enables authorized users to search records and retrieve information on the Veteran's or Service member's profile or military history; on certain education benefits; and information on compensation and disability pension ratings and awards and on dependents included in those awards. The VIS-AWS system supports customer groups throughout the entire VA. The VIS-AWS system itself stores no data; it is only a front-end user interface that accesses and searches other data repositories. Data on approximately 13 million Veterans is stored within the databases that VIS-AWS accesses. VIS-AWS performs no information sharing. It displays information extracted from other VA databases that the operator uses to support the Veteran and their dependents as needed.

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
The IT system name and the name of the program office that owns the IT system.
The Veterans Information Solution (Cloud) (VIS-AWS),
Veteran Experience Office (VEO)

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
VIS-AWS enables authorized users to search records and retrieve information on the Veteran's or Service member's profile or military history; on certain education benefits; and information on compensation and disability pension ratings and awards and on dependents included in those awards.

The VIS-AWS system does not store data; it is only a front-end user interface that accesses and searches other data repositories.

C. Who is the owner or control of the IT system or project?
IT Project Manager/System owner; Office of Information Technology

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

The VIS-AWS system itself stores no data; it is only a front-end user interface that accesses other data repositories. Data on approximately 13 million Veterans is stored within the databases that VIS-AWS accesses.

E. What is a general description of the information in the IT system and the purpose for collecting this information?
VIS-AWS is a read-only web application that displays Veteran/Service Member specific information that is utilized by the Claims examiners, Eligibility Clerks, Claims processors to determine eligibility for benefits.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.
VIS-AWS displays Veteran/Service Member's Profile, Military History, Education details, pension and disability ratings information.

G. Is 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?
VIS-AWS is a read-only Intranet application viewed via a browser and is used by users nationwide.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

A citation of the legal authority to operate the IT system.
The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

DMDC 02 DoD, Defense Enrollment Eligibility Reporting Systems (DEERS), (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02DoD.pdf (defense.gov)
https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DMDC-02-DoD.pdf?ver=2019-12-09-111827-7431

VADIR:
38VA005Q 74 FR 37093 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (7/27/2009) https://www.govinfo.gov/content/pkg/FR-2022-12-23/pdf/2022-27988.pdf

VBA Corporate:
58VA21/22/28 86 FR 61858 (11/8/2021) VA 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)

I. *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?*
No, the SORN does not require amendment, revision, or approval. Yes, the SORN for the system cover cloud usage and storage.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
The completion of this PIA will not result in circumstances that require changes to business processes.

K. *Will the completion of this PIA could potentially result in technology changes?*
The completion of this PIA will not result in circumstances that require changes to technology.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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
- ☒ 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
- ☐ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

Other PII/PHI data elements: NONE

PII Mapping of Components (Servers/Database)

VIS-AWS consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VIS-AWS 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 3.9 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**
VDRPRD VADIR-PRODUCTION (Instance: VDRPRD)	Yes	Yes	Name SSN Date of birth	Permit authorized users to view	Internal VA secure web (HTTPS

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

			Personal Mailing address Personal Phone number Personal email address Emergency contact information Race/ethnicity Military History/Service Connection	Veteran information	
VBA1 VBA Corporate Database (Instance: VBA1)	Yes	Yes	Name SSN Date of birth Military History/Service Connection	Permit authorized users to view Veteran information	Internal VA secure web (HTTPS)

1.2 What are 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?

VIS-AWS accesses VA/Department of Defense Identity Repository (VADIR), a database replicated from Defense Manpower Data Center (DMDC). .

The VIS-AWS system does not store data; it is only a front-end user interface that accesses and searches other data repositories.

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.

The VIS-AWS system does not use data from a commercial aggregator of information and no data is taken from public Web sites.

VIS-AWS is a read only viewer that displays information from VADIR (DoD replicated data), VBA Corporate database. The application business users view Veterans/ Service members military history information to determine benefits eligibility and claims processing.

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

VIS-AWS does not create information. It just displays information from VADIR (DoD replicated data) and VBA Corporate database. There are no external data sources for VIS-AWS.

1.3 How is the information collected?
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?

The VIS-AWS system is a read only internal facing web-based interface that does not store data; it only displays information from VADIR (DoD replicated data) and VBA Corporate database.

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?

VIS-AWS does not collect information on a form.

1.4 How will the information be checked for accuracy? 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.

Information is not entered into VIS-AWS. Data from the VIDIR system is searched and displayed, when the search session is complete the data is removed from the history, no data is stored in the system this is a search and display tool only.

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?

The system just displays information from the data sources (VADIR, VBA Corporate Database). System does not perform any data analysis or system accuracy checks.

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 Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk a report which contains PII is printed and removed from a controlled facility.
Mitigation: VIS-AWS does not maintain data. Only individuals who have access (approved by their leadership) can access Veteran and dependent information as required by their role. Users are trained in their responsibilities to protect and secure protected information at all times. All employees acknowledge and accept their responsibilities in safeguarding sensitive information through the VA Rules of Behavior, which also details the appropriate disciplinary action that can be expected for violating VA security policies. VIS-AWS has security controls in place that follow VA 6500 Handbook and NIST SP800-53.

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	Used to identify Veteran	Not used
Social Security Number	Used to verify the identity of the Veteran	Not used
Date of Birth	Used to verify the identity of the Veteran.	Not used
Personal Mailing address	Used to verify the identity of the Veteran.	Not used
Personal Phone Number	Used to verify the identity of the Veteran.	Not used
Personal Email address	Used to verify the identity of the Veteran.	Not used
Emergency Contact information	Used to verify the identity of the Veteran.	Not used
Race/Ethnicity	Used to verify the identity Veteran patient records	Not used
Military history/Service Connection	Used to accurately identify the Veteran for benefits processing	Not used

2.2 What types of tools are 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?

The VIS-AWS system does not conduct analysis or create data from the analyst.

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.

The system just displays information from the data sources (VADIR, VBA Corporate Database). System does not perform any data analysis or system accuracy checks or create records.

2.3 How is the information in the system 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 in transit is encrypted by the key stored in WebLogic Keystore and cannot be viewed without decrypting it. VIS-AWS is a read only viewer and does not store data and hence data at rest does not apply. Audit logs contain data in an encrypted format which cannot be accessed without decryption.

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

The VIS-AWS is a read-only application and only displays information. It does not collect PII information and displays only the last 4 of the SSN on the VIS-AWS screens. The audit logs record the application data in an encrypted format thus masking the SSNs.

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

There is no PHI data in VIS-AWS. The VIS-AWS application code is periodically scanned, and security vulnerabilities are fixed. Server infrastructure is regularly patched with updates per VA standards. These practices ensure proper security procedures are in place. VIS-AWS application is internal facing and users outside the VA firewall cannot access it. Supervisors requesting access for their employees are responsible to ensure sensitive information is appropriately safeguarded and used responsibly.

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

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:

<u>Principle of Transparency:</u> 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?

Information System Owners, in conjunction with Privacy Officers and Data Owners/System Managers, administer role-based trainings on the PII processing specific to their systems to ensure practices are consistent role-based trainings on the PII processing specific to their systems to ensure practices are consistent with notices. All ECSO employees and contractors are required to complete role-based privacy All ECSO employees and contractors are required to complete role-based privacy training on an annual basis. Training information is provided in TMS. Records Management Policy and the VA Rules of Behavior govern how Veterans' information is used, stored, and protected.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
These procedures, controls, and responsibilities regarding access are documented inside the VIS Cloud System Security Plan inside of eMass.

2.4c Does access require manager approval?

Supervisor approval is required.

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

The PII information is recorded in audit logs on the servers. All the information is in an encrypted format and cannot be accessed without decryption.

2.4e Who is responsible for assuring safeguards for the PII

The ISSO and ISO are responsible for assuring safeguards for the PII

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

VIS-AWS retains information within the operator's search queue only for the life of that session. When the user logs out, the workstation cache is flushed, and no information is retained by VIS-AWS. The information displayed may include Name, Social Security Number, Date of Birth,

Personal Mailing Address, , Personal Phone Numbers Personal Email Addresses, Emergency contact information, Race/ethnicity, Military History/Service Connection

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. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The VIS-AWS application does not retain information, it only keeps information within the operator's search queue until the next search is initiated, or until logout. When the user logs out, the workstation cache is flushed.

3.3 Has the retention schedule been 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. 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. Please work with the system Privacy Officer and 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?

The disposition authority for these records would fall under: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records Section 10, item 10

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

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records Section 10, item 10, Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule. Disposition authority: DAA-GRS 2022-0009 0001

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.

The VIS-AWS Application does not retain Veteran's personal data in the application system. VIS AWS queries two data systems (VADIR, VBA Corporate Database to meet user requests for data; once the user request has been satisfied, the data is expunged from the system. Clearing the browser cache at the end of the session is automatic.

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.

Testing is performed in the lower environments which do not have real PII information.

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 ISSO to complete all Privacy Risk questions inside the document 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: 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: The privacy risk associated with retaining PII is that it keeps information within the operator's search queue until the next search is initiated, or until logout.

Mitigation: VIS-AWS does not maintain data. Only individuals who have access (approved by their leadership) can access Veteran and dependent information as required by their role. Users

are always trained in their responsibilities to protect and secure protected information. All employees acknowledge and accept their responsibilities in safeguarding sensitive information through the VA Rules of Behavior, which also details the appropriate disciplinary action that can be expected for violating VA security policies.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Department of Veterans Affairs (VA)/Department of Defense Identity Repository (VADIR/VDRPRD).	Permit authorized users to view Veteran information	• Name • SSN • Date of birth • Personal Mailing address • Personal Phone number • Personal email address • Emergency contact information • Race/ethnicity • Military History/Service Connection	Internal VA secure web (HTTPS)
VBA Corporate database (VBA1)	Permit authorized users to view Veteran information	• Name • SSN • Date of birth • Military History/Service Connection	Internal VA secure web (HTTPS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access, which heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered by the Database personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. The access control procedures in the SSP, Monitor Logs, Supervisor approval and TMS Privacy and Information Security training (TMS 10176)

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: No external sharing.

Mitigation: No external sharing.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

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 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

DMDC 02 DoD, Defense Enrollment Eligibility Reporting Systems (DEERS), (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02DoD.pdf (defense.gov) https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DMDC-02-DoD.pdf?ver=2019-12-09-111827-7431

38VA005Q 74 FR 37093 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (7/27/2009)https://www.govinfo.gov/content/pkg/FR-2022-12-23/pdf/2022-27988.pdf

58VA21/22/28 86 FR 61858 (11/8/2021) VA 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)

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

The SORN should provide notice before collection of the information.

VIS-AWS uses the following SORN's; VADIR: Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (https://www.oprm.va.gov/privacy/systems_of_records.aspx); VBA Corporate: 58VA21/22/28 86 FR 61858 (11/8/2021) Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

6.1c 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.

VIS-AWS uses the following SORN's; VADIR: Defense Enrollment Eligibility Reporting Systems (DEERS), DMDC 02 DoD (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02-DoD.pdf (defense.gov) (https://www.oprm.va.gov/privacy/systems_of_records.aspx) VBA Corporate: 58VA21/22/28 86 FR 61858 (11/8/2021) Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

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.

VIS-AWS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems. Any notice provided would be made through those applications.

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.

VIS-AWS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems Any notice provided would be made through those applications.

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 System ISSO 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: Has sufficient notice been provided to the individual?

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

Privacy Risk: There is a risk that a Veteran may not know their information may be entered into VADIR and VBA Corporate database

Mitigation: The Veteran is informed during their transition from military service that the information they provided will be stored in systems the VA uses to adjudicate and grant/deny benefits, and additional documents will be included in those collections and protected accordingly.

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?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Access to the information displayed by VIS-AWS would be in accordance with the databases VIS-AWS accesses and would be covered in those databases PIAs.

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)?

Correction to the information displayed by VIS-AWS would be in accordance with the databases VIS-AWS accesses and would be covered in those databases PIAs.

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?

Correction to the information displayed by Cloud would be in accordance with the databases VIS AWS accesses and would be covered in those databases PIAs.

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.

Correction to the information displayed by VIS-AWS would be in accordance with the databases VIS-AWS accesses and would be covered in those databases PIAs.

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.

VIS-AWS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems. Any notice provided would be made through those applications.

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.

There is no formal redress for records displayed within the VIS-AWS; however, Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. VIS-AWS does not store any information.

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk a Veteran may not know how to obtain access to their records or how to request corrections to their records.
Mitigation: If it is determined a piece of retrieved information is incorrect, then the Veteran or VSO will have to request correction with the host database.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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?

Account requests are approved by the regional VIS-AWS coordinator, and only authorized registered individuals are granted access to the system. End users are required to follow a standard registration process managed by the Common Security Employee Manager (CSEM) system. The VA-Form 20- 8824E must be submitted to local ISO for each user. The submitting official must complete all appropriate boxes on the form identifying a specific set of user permissions. Upon complete approvals of the signed form, the form is submitted and entered into CSEM, where the information updates the Common Security Service (CSS) database to create a user profile.

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?

The applicant is registered as a system user and assigned a specific VIS-AWS user role in accordance with previously established CSS templates. All VIS-AWS users are listed in the CSS, which also serves as a documented repository of the user's sensitivity (access) level.

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.

All VIS-AWS users are listed in the CSS, which also serves as a documented repository of the user's sensitivity (access) level.

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.

Regular users of VIS-AWS are authorized VA and contractor employees. There are contractor system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not privileged users of the VIS-AWS system itself. Contracts are reviewed annually by the VIS-AWS application's Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative. Contractor personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The ROB includes non-disclosure and confidentiality agreements.

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.

A list of training for all VIS-AWS personnel required for OIT technical and business owners are maintained by system personnel and provided as eMASS evidence.

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* February 15, 2024
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* May 10, 2024
5. *The Authorization Termination Date:* May 10, 2026
6. *The Risk Review Completion Date:* September 14, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

N/A

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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

VIS-AWS does use Cloud technology. VIS-AWS uses (AWS-Amazon Web Services) Cloud from the VA Enterprise Cloud (VAEC).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Data that VIS-AWS displays is owned by VEO, and the application is owned by the system owner.

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.

Not applicable to VIS-AWS. The VAEC (VA GOV Cloud) is responsible for this if applicable.

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.

Not applicable to VIS-AWS. The VAEC (VA GOV Cloud) is responsible for this if applicable.

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

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

Not applicable to VIS-AWS. The VAEC (VA GOV Cloud) is responsible for the this if applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

ANMAR FAIK

Digitally signed by ANMAR FAIK
Date: 2024.10.01 14:25:13 -04'00'

Privacy Officer, Anmar Faik

ERIC ABRAHAM

Digitally signed by ERIC ABRAHAM
Date: 2024.10.01 14:10:27 -05'00'

Information System Security Officer, Eric Abraham

ALEXANDER TORRES

Digitally signed by ALEXANDER TORRES
Date: 2024.10.01 13:20:20 -07'00'

Information System Owner, Alexander Torres

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).

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

DMDC 02 DoD, Defense Enrollment Eligibility Reporting Systems (DEERS), (October 16, 2019, 84 FR 55293; corrected December 2, 2019, 84 FR 65975). DMDC-02DoD.pdf (defense.gov)

VADIR:
138VA005Q 74 FR 37093 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (7/27/2009) https://www.govinfo.gov/content/pkg/FR-2022-12-23/pdf/2022-27988.pdf

VBA Corporate:
58VA21/22/28 86 FR 61858 (11/8/2021) Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA
(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

HELPFUL LINKS:

Record Control Schedules:
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):
https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices