Privacy Impact Assessment for the VA IT System called:

Common Security Web Applications (CSWeb/CSAP)

Veteran Benefits Administration (VBA)

Benefits and Memorial Services (BAM)

eMASS ID # 2364

Date PIA submitted for review:

2/4/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	marvis.harvey@va.gov	(202) 461-8401
Information System Security Officer (ISSO)	Tamer Ahmed	tamer.ahmed@va.gov	215-842-2000 x2012
Information System Owner	Lindsay Tucker	lindsay.tucker@va.gov	512-364-1176

Abstract

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

Common Security Application (CSAP) is the realization of VA's effort to modernize the legacy Common Security Services (CSS) application into a single web-based interface. CSAP will reside on the Benefits Infrastructure Platform (BIP) and provide connectivity and security configuration for users of Veterans Benefit Administration (VBA) applications. Initially, CSAP will contain CSS's Common Security Employee Manager (CSEM) functionality. The CSEM functionality provides an automated approval workflow to request application and sensitive record level access, sensitive file maintenance, security logs, and inactive user management. As modernization efforts continue, CSAP will encompass the entirety of CSS to include CSEM, Common Security User Manager (CSUM), and Common Security Application Manager (CSAM) functionality. The CSUM feature grants security access to VBA client applications, sensitive file processing, and reports. The CSAM feature manages application creation, updating, and removal as well as corresponding roles, functions, services, and related restrictions.

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?

OIT. CSWeb/CSAP manages end user access via role-based application assignments as well as sensitive access level, sensitive file maintenance and relationship permissions.

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 Benefits Administration (VBA) Office of Business Integration (OBI)

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?

30,001-50,000. The typical client Benefits Application end user. This application is used to assign permissions to an end user of a VA benefits related application.

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

30,001-50,000. The typical client Benefits Application end user. This application is used to assign permissions to an end user of a VA benefits related application.

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

This application is used to assign permissions to an end user of a VA benefits related application.

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

CSWeb/CSAP does not directly share any data with any external applications, but it does consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)), VBA Corp Database and Benefits Enterprise Platform. The PII collected by these components is used for identification for user access to VA benefits systems.

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

CSWeb/CSAP is a single web application, utilizing a single database, VBA Corp. It does not directly share any data with any other or external applications. Information is shared internally for authentication and claims processing purposes. The data used is for identification for user access to VA benefits systems.

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?

This is a web application hosted in VA Enterprise Cloud Amazon Web Service GovCloud High available to authenticated users on all VA sites. The same controls are used across all sites as it is a single web application, utilizing a single database.

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

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

Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55.

VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021) the following: Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII apply.

H. What is the SORN?

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

I. SORN revisions/modification

N/A

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

The SORN will not need to be modified as it covers cloud storage and usage.

4. System Changes

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

☐ *Yes*
☒ *No*

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

☐ *Yes*
☒ *No*

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
- ☐ 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: Benefit Delivery Network (BDN) Employee Identifier Number (EIN), CSS User ID, VA Claim Number, Active Directory 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?

Information is collected from and by VA Employees/Contractors in order to assess proper permissions and access needed to internal VA systems.

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

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.

No externally facing site is used by CSWeb/CSAP as a source of information.

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

CSWeb/CSAP has the capability to generate lists of authorized users for a benefits application.

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?

VA form 8824-E is submitted to a qualified VA individual who manually inputs required data into CSWeb/CSAP directly.

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 form's agency number is VA-8824-E with no OMB control number since it is an electronic form.

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.

CSWeb/CSAP validates personal information with data in VBA Corporate Database and validates application roles and security functions requested.

Data will be checked for completeness by regular system audits performed by ISOs (Information System Officer) and directors.

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?

CSWeb/CSAP does not utilize commercial data aggregators to verify information.

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 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021) the following: Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII apply.
The official system of records notice (SORN) for "Compensation, Pension, Education, and Vocational

Rehabilitation and Employment Records-VA" (58VA21/22/28) can be found on-line at http://www.oprm.va.gov/privacy/systems_of_records.asp

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: 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: Sensitive Personal Information including personal contact information, SSN and benefit information may be released to unauthorized individuals.

Mitigation: All personnel with access to the VA network and Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. In addition to training, a security check is used to verify whether the CSS application user has the access level needed to view the Veteran's file. If the user has a sufficient level of access to view the record, the record is provided to the user. If not, access is denied and the attempt is logged, and will show up on a report provided to the Information Security Officers (ISO).

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	Individual identification/qualification assessment purposes.	Not used
SSN	Individual identification/qualification assessment purposes.	Not used
Phone Number	Individual identification/qualification assessment purposes.	Not used
Email Address	Individual identification/qualification assessment purposes.	Not used
CSS User ID	Individual identification/qualification assessment purposes.	Not used
Benefit Delivery Network (BDN) Employee Identifier Number (EIN),	Individual identification/qualification assessment purposes.	Not used
VA Claim Number	Individual identification/qualification assessment purposes.	Not used
Date of Birth	Individual identification/qualification assessment purposes.	Not used

Active Directory Data	Individual identification/qualification assessment purposes.	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?
Data will be checked for completeness by regular system audits performed by ISOs (Information System Officer) and directors. No new data is created during analysis. CSWeb/CSAP provides lists of qualified users for benefits applications.

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.

CSWeb/CSAP allows an authorized user to add a record for a brand new VA end user, as well as records that represent the application access, sensitivity, and level permissions.

2.3 How is 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?

While in transit, systems use mutual SSL and authentication encryption protocols. All data is encrypted at rest and during transit.

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).

All SSNs are encrypted at transit and at rest.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
All Users, employees, and contractors are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

All Users, employees, and contractors are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

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?

Users are trained how to handle sensitive information by taking VA Privacy and Security Awareness Rules of Behavior training (mandatory for all personnel with access to sensitive information or access to VA network). After completing the course, users read and attest they understand the VA Rules of Behavior.

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?

Yes. The controls in place, ensuring that information is handled properly are as follows: The minimum security requirements for CSWeb/CSAP's moderate impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. All security controls in the respective moderate impact security control baseline are employed unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

2.4c Does access require manager approval?

Yes.

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

Yes.

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

CSWeb/CSAP does not store or maintain PII; SSNs are collected by CSWeb/CSAP for storage *in eMASS?*the VBA Corporate Database. The ISSO is required to perform audits by crosschecking permissions approved on the VA FORM 20-8824E (Access form) against the actual permission entered into CSWeb/CSAP. Any change to individual records would have to be made by contacting their VBA Regional Office.

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

CSWeb/CSAP does not retain any 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. **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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

CSWeb/CSAP does not retain any data.

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?

CSWeb/CSAP does not retain information. The VBA Corporate Database (eMASS #2313) (different VASI and eMASS ID) stores all pertinent records.

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

All data is retained permanently in the VBA Corporate Database and follows the NARA General Schedule. The National

Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. The retention period is a minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach are to be maintained for 6 years (HIPAA requirement). Please see SORN 58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.

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.

All CSWeb/CSAP data is stored in the VBA Corporate Database. The elimination of SPI is not handled by CSWeb/CSAP.

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.

Access to data containing PII must go through an approval process that requires signatures from Supervisors/CORs and Directors. Other users not requiring access to PII data can use CSEM and CSUM in test environments which only contain mock data.

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 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 contained in the system will be retained for longer than is necessary to fulfill the VA mission; however, this risk would fall upon the accreditation boundary of the VBA Corporate Database since the PII is maintained within it, not CSS itself. The Privacy Risk and Mitigation noted in the CRP Privacy Impact Assessment dated 05-29-2015 states:
As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

Mitigation: Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII or PHI which may appear in the data and files collected.

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 CSWeb/CSAP consists of 2 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 CSWeb/CSAP 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,	Does this system collect PII? (Yes/No)	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

Application Program Interface (API) etc.) that contains PII/PHI		**PII? (Yes/No)**			
VBA Corporate Database (eMASS ID# 2313)	Yes	Yes	Name, SSN, Phone Number, VA Email Address, CSS User ID, Benefit Delivery Network (BDN) Employee Identifier Number (EIN), VA Claim Number.	The data is used for identification for user access to VA benefits systems.	HTTPS using Secure Socket Layer encryption certificate.
Benefits Enterprise Platform (eMASS #2237)	Yes	Yes	Name, SSN, Phone Number, Email Address, CSS User ID, Benefit Delivery Network (BDN) Employee Identifier Number (EIN), VA Claim Number,	The data is used for identification for user access to VA benefits systems.	HTTPS using Secure Socket Layer encryption certificate.

			VA Email Address.		

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***
VA AD Service	This information is shared for authentication and claims processing purposes.	Active Directory Data	HTTPS (Internal)
VBA Corporate Database (CRP), eMASS ID# 2313	This information is shared for authentication and claims processing purposes.	Bidirectional First, Middle, and Last Name, DOB, Address, Phone Number, SSN, VA Email Address	JDBC

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*
BIP Security Service (BSS), eMASS ID# 2047	This information is shared for authentication and claims processing purposes.	Bidirectional First, Middle, and Last Name, VA Email, Application and Authorities	HTTPS (Internal)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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: Sharing of protected Veteran data is necessary to support VA benefits processing/ensure eligible Veterans receive the VA benefits to which they are entitled; however, sharing of any information carries with it a risk of unauthorized disclosure.

Mitigation: The risk of improperly disclosing protected Veteran data to an unauthorized internal VA entity and/or VA personnel is mitigated by limiting access only those VA entities and personnel with approved access and clear business purpose/need to know. Additionally, consent for use of PII data is signaled by the completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. Information is shared in accordance with VA Handbook 6500.

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.

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.

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 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: The VA cannot control what the VSOs, SAAs, and VA accredited attorneys or claims agents do with the data they view, after they view it; therefore it could potentially be shared with entities and individuals without proper permissions to access the data; however, that risk would fall on the application through which the user was accessing that is stored within the VBA Corporate Database, not on CSWeb/CSAP, itself. CSWeb/CSAP does not store or maintain PII.

Mitigation: QRadar produces audit logs of the VBA Corporate Database which is where all PII for CSWeb/CSAP is stored. ISOs also review records in the sensitive record file, at least every 3 years. All external entities access the data from an internal VA account, behind the VA firewall. Privacy is further secured by storing all data on encrypted local servers behind firewalls and external users are vetted and trained in the same exact manner as VA employees.

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.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.

Notice is provided under SORN 58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021 24372.pdf and the publishing of this document.

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

Notice is provided under SORN 58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021 24372.pdf and the publishing of this document.

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

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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.

All information in CSWeb/CSAP is collected from VA Employees. As all information collected is related to individual qualification, individuals do not have a right to decline to provide information and as such there is no penalty attached.

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.

Information is collected from VA employees and contractors to configure system access for assigned duties and responsibilities. As such, no consent for specific uses of data can be provided nor is it needed.

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: Privacy information may be collected prior to providing the written notice to the veteran or employee. The public may not be aware the CSWeb/CSAP system exists and the purpose for the CSWeb/CSAP system.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. Notice is provided, primarily, via the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

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.***

Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. See VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021)

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)?

CSWeb/CSAP 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?

CSWeb/CSAP is not exempt from the access provisions of the Privacy Act.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1,

state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The correction of inaccurate or erroneous information would not occur within CSWeb/CSAP, itself, as CSWeb/CSAP does not store any PII or SPI. All data is stored in the VBA Corporate Database.

The Individuals seeking information regarding access to and contesting of VA records at the source system may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. See VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021).

CSWeb/CSAP Administrators and ISO have access to all CSWeb/CSAP data. The end user access is restricted by the level of authority they require to perform their jobs. The CRP/BEP Customers include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. The only authorized users (routine-user) are the System Administrator and the Information System Security Officer (ISSO).

The SSN is used only for internal identification purposes. Usually, it is the ISSO who is first to notice a situation where the SSN or VA Claim Number in CSS does not match the access request form. ISSOs have "read-only" access. Administrators cannot modify their own security record. In no situation would the end-user for which the security record was created have access to their security record.

The ISSO is required to perform audits by crosschecking permissions approved on the VA FORM 20-8824E (Access form) against the actual permission entered into CSWeb/CSAP. Any change to individual records would have to be made by contacting their VBA Regional Office.

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.

CSWeb/CSAP does not store or maintain any PII or SPI. All PII and SPI is housed within the VBA Corporate Database and is not part of the CSWeb/CSAP application's accreditation boundary. Therefore, VBA application that contains the Veteran's record would provide instruction regarding record correction. Once the Veterans information is corrected within the appropriate VBA application the information would be updated in the VBA Corporate Database. VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021), states:

"Records Access Procedures Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. The list of VA regional offices referenced in the SORN can also be found at:

http://benefits.va.gov/benefits/offices.asp."

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.

Users can visit a VBA Regional Office, the VBA Internet Site, or call 1-888-442-4551 for assistance with this process.

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.

Principle of Individual Participation: 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.

Principle of Individual Participation: 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:

Privacy Risk: This risk would fall on the VBA application to which the user is trying to access. CSWeb/CSAP itself does not store any PII or SPI. All sensitive data is transmitted to VBA Corporate Database for storage.

Mitigation: VA, SORN 58VA21/22/28 (November 8, 2021) states that individuals should contact their local VA Regional Office for additional information about accessing and contesting their records at the VA.

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?
Applicants must request access electronically using CSWeb/CSAP. A series of verification and approval levels are set up to ensure the applicant's information is valid and management approves of the access.

Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and electronic signs he/she will abide by the VA Rules of Behavior. The user also must complete mandatory security and privacy awareness training. CSS Administrators and ISSO have access to all CSS data. The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. The only authorized users (routine-user) are the System Administrator and the Information System Security Officer.
The SSN is used only for internal identification purposes. Usually, it is the Information Security Officer who is first to notice a situation where the SSN or VA Claim Number in CSS does not match BIRLS or the access request form. ISSOs have "read-only" access. Administrators cannot modify their own security record.

In no situation is the end-user for which the security record was created would ever have access to their security record.

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?
External Agencies and their personnel do not have access to CSWeb/CSAP in any capacity.

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.

- Initiator: Requests access to one or more applications that use VBA data from source documentation and use the information on the documentation to enter the request in CSWeb/CSAP. Functions used: Add Employee, Update Username, Application Request, Level Request

- Approving Official: Reviews a submitted request in their queue to approve or deny this request. The approving official is the first line approver.

Functions include: Manage Employee, Application Request, Level Request

- Director: Reviews a submitted request in their queue to approve or deny this request. The director is the final approver. Functions include: Manage Employee, Application Request, Level Request

- Implementer: Applies approved requests for user access changes. Functions include: Application request, Manage employee, Manage Divisions, Manage Sensitivity, Level Request, Manage Inactive Users, Reports

- Auditor: Views requests to ensure appropriate access. They also check reports for mandated security reviews. Functions include: View Application Request, View Division Management, Reports

- Super User: Provide triage and support for questions and issues. This role is limited to only a few people. Functions include: Manage Employee, Manage Divisions, Manage Sensitivity, Level Request, Manage Inactive Users, Reports

- Restricted Portfolio Management (RPM) Team: Specialty business team that assists customers and manages inactive users. Functions include: Level Request, Manage Inactive Users, Reports

- Administrator: Maintain selection lists and restrictions for applications, functions, and roles. Functions include: Manage Values.

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

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

8.2c. Does the contractor have a signed confidentiality agreement?

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

VA contractors do not have access to the CSWeb/CSAP production environment and all PII is stored in the VBA Corporate Database, which is not part of the CSWeb/CSAP accreditation boundary. The contractors that work on the VBA Corporate Database are vetted as follows:

• VBA VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system.

• Contractor access is reviewed annually at a minimum

• The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS).

• All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role.

• Contractors with system administrative access are required to complete additional role-based training prior to gaining system administrator access.

• Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information System Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition.

• Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behaviors (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all VA personnel must complete via the VA's Talent Management System (TMS).

After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgement and is tracked through the TMS system. CSWeb/CSAP users must also complete annual Privacy and Security training.

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

No.

8.4a If Yes, provide:

1. *The Security Plan Status:* In Progress
2. *The System Security Plan Status Date:* In Progress
3. *The Authorization Status:* In Progress
4. *The Authorization Date:* In Progress
5. *The Authorization Termination Date:* In Progress
6. *The Risk Review Completion Date:* In Progress
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.***

Development is complete for initial operating capability and UAT successful as of August 9th, 2024. But cannot actually go live in Production until receive Minor approval.

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)***

CSWeb/CSAP utilizes the AWS VAEC GovCloud.

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.*

This is not applicable to CSWeb/CSAP.

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.

This is not applicable to CSWeb/CSAP.

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.

This is not applicable to CSWeb/CSAP.

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).

This is not applicable to CSWeb/CSAP.

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.

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2025.04.07 13:35:32 -05'00'

Privacy Officer, Marvis Harvey

TAMER AHMED

Digitally signed by TAMER AHMED
Date: 2025.04.07 14:11:57 -04'00'

Information System Security Officer, Tamer Ahmed

LINDSAY TUCKER

Digitally signed by LINDSAY TUCKER
Date: 2025.04.07 10:29:01 -05'00'

Information System Owner, Lindsay Tucker

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).

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

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)