Privacy Impact Assessment for the VA IT System called:

Web Enabled Approval Management System

VBA – Veterans Benefits Administration

Enterprise Program Management Office

eMASS ID 133

Date PIA submitted for review:

November 4, 2024

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)	Sharon Gainey	Sharon.Gainet@va.gov	914-441-4019
Information System Owner	Warren Majors	Warren Majors@va.gov	630-414-3250

Abstract

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

Web Enabled Approval Management System (WEA) is comprised of 4 applications – Web Enabled Approval Management System (WEAMS), WEAMS Public, Work Study Management System (WSMS), and Flight, On-the-Job Training, Correspondence, Apprenticeship System (FOCAS). WEA manages the information for all programs and facilities approved for delivering training under the VA educational programs. WEA supports the processing of Work Study claims, tracks payments, and is used for managing contracts between VA and claimants. Additionally, WEA sends award payment information to BDN for processing.

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?

WEA is comprised of 4 applications – Web Enabled Approval Management System (WEAMS), WEAMS Public, Work Study Management System (WSMS), and Flight, On-the-Job Training, Correspondence, Apprenticeship System (FOCAS). WEAMS is an internal web-based application designed to oversee all programs and facilities approved for delivering training under the VA educational programs (Education and Vocational Rehabilitation and Employment). WEAMS Public is an external web-based application available for use on the Internet by veterans and beneficiaries to search for and view VA approved colleges, universities, license and certifications, and national exams. The application provides addresses of the institution, programs offered by the institution, and certified official information. WSMS is an internal web-based application designed to maintain information on Work Study applications for veterans and their dependents. The application supports the processing of Work Study claims, tracks payments, and is used for managing contracts between VA and claimants. FOCAS is an internal web-based application designed to send award payment and fiscal activities to BDN for processing. This covers Chapter 30, Chapter 1606 and Chapter 1607 educational benefits for Veterans who pursue training in FOCAS awards programs.

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.

VA Owned and VA Operated.

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?

40,000

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

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

WEAMS and WEAMS Public does not collect, process, retain or share any information about individuals. WSMS and FOCAS collects and processes Social Security Number, File Number, First Name, Last Name, Address, and Phone to support the processing and tracking of claims and payments. The PII is stored in the VBA Corporate Database (CRP).

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

WSMS and FOCAS information is stored in the VBA Corporate Database (CRP) – Database (CorpDB) and shared with the Benefits Delivery Network (BDN).

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

Yes. WEAMS and WEAMS Public does not collect process, retain or share any information about individuals. WSMS and FOCAS collects and processes information.

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?

WEAMS Public is operated at the Philadelphia Information Technology Center (PITC) and does not process PII. WEAMS, WSMS, and FOCAS are operated at the Austin Information Technology Center (AITC).

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?

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).

I. SORN revisions/modification

FR Doc. 2021–24372 Filed 11–8–21; 8:45 am

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

WEA is not in the process of being changed; however, the system authorized to store WEA data is scheduled to migrate to the cloud in FY2025.

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
- ☐ Gender/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☐ Other Data Elements (list below)

Other PII/PHI data elements: File number.

1.2 List the sources of the information in the system

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

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

The information is collected from the application for Work Study, VA form 22-8691. However, because Work Study is a supplemental benefit that can only be awarded if the claimant is using a VA education benefit, VA also utilizes SHARE to confirm SSN/ File Number. Additionally, we may use other Education programs to confirm name or phone number if needed.

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.

WSMS pulls all claimant data from SHARE. Additionally, the system pulls school facility codes from WEAMS. For reporting purposes, WSMS data feeds into OBIEE and exports from there for needed information.

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

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

Web Enabled Approval Management System (WEA) does not create information.

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?

Web Enabled Approval Management System (WEA) stores information listed in Section 1,1 in the VBA Corporate Database (CRP) transmitted electronically from WSMS and FOCAS applications for the processing and tracking of claims and payments.

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?

Web Enabled Approval Management System (WEA) does not collect information on a form. The information is collected electronically.

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.

WSMS uses SHARE to check for accuracy. Additionally, quality checks are performed by the Education Quality Specialist Team to do random reviews per employee each month.

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?

Web Enabled Approval Management System (WEA) does not check for accuracy by accessing a commercial aggregator of 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

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). Legal authority to maintain the system is: Title 10 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.

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: If the information collected by Web Enabled Approval Management System (WEA) stored in VBA Corporate Database (CRP) was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is processed by the system.

Mitigation: All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness and Rules of Behavior Training annually. All data is encrypted in transit to the database and at rest in the database. SSNs are protected via least privilege RBAC (rules-based access control). Data is also protected via the implementation of Sensitivity Levels, whereby users must be granted specific Sensitivity levels from the Web Enabled Approval Management System (WEA) ISSO to see specific information.

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
Social Security Number	To identify the Veteran and/or claimant	Not used
File Number	To identify the Veteran and/or claimant	Not used
First Name	To identify the Veteran and/or claimant	Not used
Last Name	To identify the Veteran and/or claimant	Not used
Address	To correspond with the Veteran and/or claimant	Not used
Phone	To correspond with the Veteran and/or claimant	Not used

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

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

Data is checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the Veteran is receiving. Also, data are updated with each Veteran correspondence. Data are updated because of returned mail, or returned direct deposits, or through contact with the Veteran, beneficiary, or power of attorney. All data are matched against supporting claims documentation submitted by the Veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the Veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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.

WEA does not create or make available new or previously unutilized information about an individual.

2.3 How the information in the system is secured.

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

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

Encryption is used for data in transit and for data at rest.

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).

SSNs are protected via least privilege RBAC (rules-based access control). Data is also protected via the implementation of Sensitivity Levels, whereby users must be granted specific Sensitivity levels from the Web Enabled Approval Management System (WEA) ISSO to see specific information. The data is stored and encrypted at rest in the in the VBA Corporate Database (CRP).

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.

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?

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

2.4a How is access to the PII determined?

Web Enabled Approval Management System (WEA) has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 and VA directives or handbooks based on the Control Attributes impact of Moderate and the Privacy overlay including 26 Control families to protect the confidentiality, integrity, and availability of the information processed, stored, and transmitted by the system. The control families include Access Control; Accountability, Audit, and Risk Management; Audit and Accountability; Authority and Purpose; Awareness and Training; Configuration Management; Contingency Planning; Data Minimization and Retention; Data Quality and Integrity; Identification and Authentication; Incident Response; Individual Participation And Redress; Maintenance; Media Protection; Personnel Security; Physical and Environmental Security; Planning; Program Management; Risk Assessment; Security; Security Assessment and Authorization; System and Communications Protection; System and Information Integrity; System and Services Acquisition; Transparency; and Use Limitation. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans' information is used, stored, and protected.

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

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 in eMASS?

Web Enabled Approval Management System (WEA) Information System Owner (ISO), Information System Security Officer (ISSO), and Privacy Officer (PO).

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*

Web Enabled Approval Management System (WEA) collects and processes but does not retain any information. All data from Section 1 is stored within VBA Corporate Database (CRP), which is beyond the scope of Web Enabled Approval Management System (WEA).

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.*

Web Enabled Approval Management System (WEA) collects and processes but does not retain any information. All data from Section 1 is stored within VBA Corporate Database (CRP), which is beyond the scope of Web Enabled Approval Management System (WEA). The CRP retains the data indefinitely.

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?

Web Enabled Approval Management System (WEA) collects and processes but does not retain any information. All data from Section 1 is stored within VBA Corporate Database (CRP), which is beyond the scope of Web Enabled Approval Management System (WEA). The CRP retains the data indefinitely with an approved disposition authority.

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

Web Enabled Approval Management System (WEA) collects and processes but does not retain any information. All data from Section 1 is stored within VBA Corporate Database (CRP), which is beyond the scope of Web Enabled Approval Management System (WEA). The CRP retains the data indefinitely with an approved disposition authority. All data is retained permanently and follows the NARA General Schedule. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Please see SORN 58VA21/22/28 86 FR61858 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.

Web Enabled Approval Management System (WEA) collects and processes but does not retain any information. All data from Section 1 is stored within VBA Corporate Database (CRP), which is beyond the scope of Web Enabled Approval Management System (WEA).

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.

Web Enabled Approval Management System (WEA) does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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 is within VBA Corporate Database (CRP) since the PII is retained within VBA Corporate Database (CRP) and not within Web Enabled Approval Management System (WEA).

Mitigation: Retention of information is regulated and managed via the NARA General Records Retention Schedule; however, mitigation of this risk is the responsibility of VBA Corporate Database (CRP).

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 Web Enabled Approval Management System (WEA) consists of one 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 Web Enabled Approval Management System (WEA) and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
VBA Corporate Database (CRP) – Database (CorpDB)	Yes	Yes	SSN, File Number, First Name, Last Name, Address, Phone	Support the processing and tracking of claims and payments.	All Users, employees, and contractors are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

					Privacy overlay applied to the system. Related controls enforced. HTTPs protects data in transit and encryption protects data at rest.

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***
VBA Corporate Database (CRP)	WSMS and FOCAS stores collected data in the database.	Social Security Number File Number First Name Last Name Address Phone	HTTPS using Secure Socket Secure Socket Layer encryption certificate.
Benefits Delivery Network (BDN)	To process Veteran claims.	Social Security Number File Number First Name Last Name Address Phone	Manually entered by user

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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 personnel is mitigated by limiting access only those VA entities and personnel with approved access and clear business purpose with a need to know. 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: There is no privacy risk since Web Enabled Approval Management System (WEA) does not share any data externally.

Mitigation: There is no mitigation required since Web Enabled Approval Management System (WEA) does not share any data externally.

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.

Notice is provided under 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

6.1b If notice was not provided, explain why.

The Privacy Notice is provided.

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

Notice states VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service Members, Reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA. See the statutory provisions cited in ''Authority for maintenance of the system.'' Notice is provided under 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

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

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

The information is required to receive the benefit from the VA. The Privacy Act and Respondent Burden information is provided to the individual.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The Privacy Act and Respondent Burden information is provided to the individual.

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: An individual may not receive notice that VBA Corporate Database (CRP) is processing their information.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in 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. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 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)?

Web Enabled Approval Management System (WEA) 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?

Web Enabled Approval Management System (WEA) is a Privacy Act system.

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

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

Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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.

Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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.

Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/2886 FR 61858 (November 08, 2021).

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: There is a risk that individual may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and files. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and files.

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?

User authentication for WEA internal applications is managed and performed by VA Common Security Services (CSS). Each user is required to enter his/her station ID (linked to a RO), user ID, and PIV Login/PIN thru the CSS authentication interface.

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?

Users from other agencies do not have access to the internal WEA applications.

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.

Each WEA application defines the different roles that allow user to perform their assigned duties. WEA documents and implements the concept of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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

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

Contractors are involved in the maintenance of the system.

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

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

WEA does not process 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.

OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter. 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 systems 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, ISSO, 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 ROB or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. VA employees and 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). The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session. All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems 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, ISSO, 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.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 05/16/2024
3. *The Authorization Status:* Authorized to Operate
4. *The Authorization Date:* 07/16/2023
5. *The Authorization Termination Date:* 07/15/2025
6. *The Risk Review Completion Date:* 06/16/2023
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.***

Web Enabled Approval Management System (WEA) has completed A&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. ***(Refer to question 1.8 of the PTA)***

Web Enabled Approval Management System (WEA) does not use cloud technology.

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.*

Web Enabled Approval Management System (WEA) does not use cloud technology.

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.

Web Enabled Approval Management System (WEA) does not use cloud technology.

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.

Web Enabled Approval Management System (WEA) does not use cloud technology.

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).

Web Enabled Approval Management System (WEA) does not use RPA technology.

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: 2024.11.20 06:14:00 -06'00'

Privacy Officer, Marvis Harvey

SHARON GAINEY

Digitally signed by SHARON GAINEY
Date: 2024.11.22 09:28:57 -06'00'

Information System Security Officer, Sharon Gainey

WARREN MAJORS

Digitally signed by WARREN MAJORS
Date: 2024.11.22 09:46:35 -06'00'

Information System Owner, Warren Majors

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).

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)