Privacy Impact Assessment for the VA IT System called:

EDU Philadelphia Information Technology Center (EDU PITC) Web Applications

Education Service – Education Veteran Readiness and Employment Product Line VBA

Date PIA submitted for review:

07/25/2023

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Bertha Brown	Bertha.Brown@va.gov	202-461-9740
Information System Security Officer (ISSO)	Mark Ingold	Mark.Ingold@va.gov	918-310-4684
Information System Owner	Darla van Nieukerk	Darla.vanNieukerk@va.gov	202-802-8636

Abstract

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

EDU Philadelphia Information Technology Center (EDU PITC) Web Applications is a collection of Web-enabled distributed applications delivering educational services to users on the Internet. Customers include: Educational Organizations, Veteran Students, Training Facilities, and Educational Liaison Representatives, Intranet Veteran Customer Service Representatives, and Central Office (CO)/Regional Processing Office (RPO) personnel.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.
EDU Philadelphia Information Technology Center (EDU PITC) Web Applications, Education Service, Veterans Benefits Administration (VBA).

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
Allows GI Bill claimants to electronically complete and transfer monthly verification of attendance, along with student status changes to Education Regional Processing Offices to release monthly payments.

C. Indicate the ownership or control of the IT system or project.
VA Owned and VA Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
The expected number of individuals whose information is stored in the system is approximately 229,589. The typical client or individuals are students.

E. A general description of the information in the IT system and the purpose for collecting this information.

Each Education Web subsystem (application) supports the goal of delivering Education services.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions. WAVE Internet Application allows students to electronically complete and transfer monthly verifications of enrollment and student status changes to Education Regional Processing Offices to release monthly payments. It also completes and transfers monthly verification of enrollment and student status changes. Students can also submit changes of address and Direct Deposit information via this system in a secure environment using secure sockets (SSL) layer certificate.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The EDU system is hosted and located at Philadelphia Information Technology Center (PITC) EDU Web Applications include WAVE. See section 1.1 for additional information.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. SORN 58VA21/22/28 states: Authority For Maintenance of 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.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

N/A

4. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No change to the business processes.

K. Whether the completion of this PIA could potentially result in technology changes

No changes to the technology

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below: relationship to Veteran, Education Data)

PII Mapping of Components (Servers/Database)

Education Web Applications - EO Application code (EDU) consists of **two** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Education Web Applications - EO Application code (EDU)** 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 the server names in the table.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Wave (Production) database Wave (Preproduction) database	Yes	Yes	• Name SSN • DOB • Personal Mailing Address • Zip Code • Phone Number(s) • Relationship to veteran • Education Data • Service information • E-Mail Addresses • Financial Account • IP	Completes and transfers monthly verification of enrollment and student status changes. Change of address and direct deposit information	Data base encrypted; SSL Connections enforced; Software Code Review/WASA scan/NSOC scan

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Veterans and their eligible dependent provides specific information to complete application for Education benefits using VA form 22-1990.

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.

N/A

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

N/A

1.3 How is the information collected?

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

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

EDU Web Applications can accept claims from several sources: mail, fax, email which will provide submission of a claim application through the Internet. Paper claims and other documents received are scanned into the system and stored into the appropriate veteran's eFolder. The SPI information is collected via electronic transmissions from the master VBA repositories (Corporate, Beneficiary Identification and records Locator System (BIRLS), Benefit delivery Network) and Master Databases (BDN) Forms utilized are VA Forms 22-1999, 22-1999b, and 22-6553c. WAVE is used by Veterans only.

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

Forms utilized are VA Forms: 22-1990, 22-1990e, 22-1990n, 22-1990t, 22-1999, 22-199b and 22-6553c

1.4 How will the information be checked for accuracy? How often will it be checked?

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

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

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

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. The correspondence with each veteran is then used

to update the data. All collected data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as Social Security Number (SSN) is verified with VBA. 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. The WAVE data is crossed checked against military records and other government sources at regional processing centers.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment. 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs. SORN 58VA21/22/28 states 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 is the
authority for maintaining the system.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk in providing submission of a claim application through the Internet. Paper claims and other documents containing SPI, PII and or PHI received are scanned into the system and stored into the appropriate veteran's eFolder. This could put the privacy data of individuals at risk of being inappropriately shared.

Additionally, EDU collects Personally Identifiable Information (PII) and other highly delicate Protected Health Information (PHI). If this information 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 contained in the system.

Mitigation:

- EDU adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- All employees with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

The intended use of the veteran and veteran's family (spouse, children, parents, etc.) information is to determine eligibility and entitlement for VA education benefits:

- Social Security Number (SSN)- used to positively identify individual requesting/ receiving benefits.
- Name- To identify the Veteran –internal/external
- Mailing Address- For communication with the Veteran –internal/external
- Zip Code- Part of mailing address –internal/external
- Phone Number(s)- For communication with the Veteran–internal/external
- E-Mail Addresses- For communication with the Veteran–internal/external
- Data of Birth - used to positively identify individual requesting/ receiving benefits internal/external
- Financial Account Information – To send direct deposits to Veteran–external

- IP Address – web server logs/general connections; not used in any processing.
- Relation to Veteran- To identify relationship status.
- Educational Data- To identify level of education

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.
N/A, EDU/WAVE does not analyze data and no additional data is produced

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.

This description of tools that are utilizes to analyze data is provided below:

Education Web Applications is a collection of Web-enabled distributed applications delivering 66 educational services as front-end tool allowing users to initiate request for education benefits and does not fully integrate with business lines' back-end systems supplying those education benefits.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
Data in transit is protected by SSL, HTTPS, and SFTP transfer. Data at rest is encrypted with Microsoft Transparent Data Encryption (TDE)

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

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Data in transit is protected by SSL, HTTPS, and SFTP transfer. Data at rest is encrypted with Microsoft Transparent Data Encryption (TDE)

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? A potential user uses their Name, SSN, and VA File Number (if available) to log into the website. The website verifies said information against a BDN data import, containing the information of WAVE eligible users.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

All accounts come from a BDN feed.

2.4c Does access require manager approval?

System level access does.

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

Yes, system audit user access via Splunk, BigFix, etc.

2.4e Who is responsible for assuring safeguards for the PII?
PITC System Administrators.

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*

EDU Web Applications retains SPI information (Name, Social Security Number, Date of Birth, Personal mailing address, Personal Phone Number(s), Personal Email Address, Financial Account Information, Internet Protocol (IP) Address Number.)

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

WAVE data is retained for 60 days.

Currently the retention period on documents set to "0", documents never get deleted. This allows students information to remain in the system if they decide to re-enroll in school again.

In order for the EDU Web Applications to become of a system of record, the requirements were structured to adhere to the paper retention requirements previously existing for these records.

If EDU systems were to be decommissioned data would be transferred to a replacement system.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. 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?

Yes

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

- VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA
- Compensation, pension and Vocational Rehabilitation, Records Control Schedule VB-1 Part 1 Section XIII as authorized by NARA
- Education – Regional Processing Office, Record Control Schedule VB-1, Part 1, Section VII as authorized by NARA

https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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.

Data is not eliminated. It is controlled in accordance with NARA control schedules determined by the agency involved. NARA controls schedules have a termination date unless it falls under special regulations and becomes a permanent VA record such as presidential items, items unique to history, etc. Otherwise at some point the data will be destroyed. VA Handbook 6300.1Records Management Procedures explains the Records Control Schedule (RCS) procedures. Operating units will be in compliance with VA policy.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission or reaching date approved by NARA Records schedule), will be carried out in accordance with VA Handbook 6500.1 Electronic Media Sanitization.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Any temporary records such as working copies in paper form will be destroyed in accordance with NARA approved RCS following VA Directive 6371.

Items in the system are not printed; they are received electronically and placed in Education's electronic folder- The Image Management System (TIMS). Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data.

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 test environments that has PII is restricted to developers whose privileged access has been approved by EPAS. They are also required to fill out a VA-9957 (Access Form) and submit confirmation of Privacy and IT Role Based Training. In addition, actual access it controlled via Two Factor Authentication, utilizing an e-token.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: 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.

To mitigate the risk of breach, access to the EDU system is controlled to only personnel with a clear business need for the data. A permission hierarchy is applied to access requests with several layers of approval before access is granted.

The principle of need-to-know is strictly adhered to by EDU personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
TIMS - The Image Management System	To identify the veteran or beneficiary	Name, Social Security, Number, Mailing Address, Zip Code, Phone	Secure File Transfer Protocol (SFTP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	using/requesting educational services	Number(s), Relationship to veteran, Education data, Service information, E-Mail Addresses	
Benefits Delivery Network (BDN)	To identify the veteran or beneficiary using/requesting educational services	Name, Social Security Number, Mailing Address, Zip Code, Phone Number(s), Relationship to veteran, Education data, Service information, E-Mail Addresses	Secure File Transfer Protocol (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: All VBA employees may use information contained in VHA records when they need the records in the official performance of their duties for benefit payment operations purposes. VBA employee may need other legal authority to use PII in the performance of official duties relates to security, research, education reporting and many other purposes as outlined in the handbook.

The privacy risk associated with transmitting PII within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation: Minimum Necessary Standard for PII requires all workforce members to be assigned a functional category so they are aware of the level of access permitted in the performance of their official duties. Per the VA 6500 handbook, VA personnel must not access information that exceeds the limits described for their functional category or job duties. The principle of need-to-know is strictly adhered to by EDU personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission. Normal standard measures are followed.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Not applicable.
There is minimal to no privacy risk as EDU does not share data external of the VA boundary.

Mitigation: Not applicable.

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Information comes from a BDN feed.

Veterans and/or beneficiaries applying for Education benefits must complete an application, VA Forms: 22-1990, 22-1990e, 22-1990n, 22-1990t, 22-1999, 22-199b and 22-6553c. The aforementioned forms include the Privacy Act Notice in the section labelled "Request to Opt Out of Information Sharing with Education Institutions."

Privacy Act Notice: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or title 38, Code of Federal Regulations, section 1.576 for routine uses (e.g., VA sends educational forms or letters with a veteran's identifying information to the veteran's school or training establishment to (1) assist the veteran in the completion of claims forms or (2) for the VA to obtain further information as may be necessary from the school for the VA to properly process the veteran's education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, and published in the Federal Register. Your obligation to respond is required to obtain or retain education benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law enacted before January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine the maximum benefits under the law. While you do not have to respond, VA cannot process your claim for education assistance unless the information is furnished as required by existing law (38 U.S.C. 3471). The responses you submit are considered confidential (38 U.S.C. 5701). Any information provided by applicants, recipients, and others may be subject to verification through computer matching programs with other agencies.

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

All users must complete an application with Privacy notice to establish a claim. A claim must be established before the VA contact the Department of Defense to confirm military service to establish eligibility.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1) The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (February 14, 2019). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf.

2) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment] publicly available through the website of the agency, publication in the Federal Register.
Notice is also provided when individuals apply for education benefits using VA Forms: 22-1990, 22-1990e, 22-1990n, 22-1990t, 22-1999, 22-199b and 22-6553c.

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

Yes, Veterans and their families have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA a SSN.

Education Benefits application includes Privacy Notice which provides instructions on how to decline by completing VA Form 22-0993, Request to Opt-Out of Information Sharing with Educational Institutions. In addition, the user is informed their application cannot be processed further.

Privacy Act Notice: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or title 38, Code of Federal Regulations, section 1.576 for routine uses (e.g., VA sends educational forms or letters with a veteran's identifying information to the veteran's school or training establishment to (1) assist the veteran in the completion of claims forms or (2) for the VA to obtain further information as may be necessary from the school for the VA to properly process the veteran's education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, and published in the Federal Register. Your obligation to respond is required to obtain or retain education benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law enacted before January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine the maximum benefits under the law. While you do not have to respond, VA cannot process your claim for education assistance unless the information is furnished as required by existing law (38 U.S.C. 3471). The responses you submit are considered confidential (38 U.S.C. 5701). Any information provided by applicants, recipients, and others may be subject to verification through computer matching programs with other agencies.

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.

Education Service takes completion and signature of the Education Benefits Application as part of Privacy Act.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: There is a risk that members of the public may not know that the Education Web Applications (EDU) exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer***

satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, Regional Office Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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).

This application is not exempt from Privacy Act.

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

The application is a Privacy Act application.

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

The procedure for correcting information is outlined in this PIA, and SORN 58 VA 21/22/28. Formal redress is provided. All information correction must be taken via the Amendment process.

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.

Formal redress is provided. All information correction must be taken via the Amendment process. In addition, the individual may contact any Regional Office for guidance on how to gain access to his or her records and seek corrective action through the Amendment 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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: The individual may not be aware of how to access, redress or correct their information.

Mitigation: The procedures to correct or amend information is included in the applicable SORN 58 VA 21/22/28, and this PIA. Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

Section 8. Technical Access and Security

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

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

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

8.1a Describe the process by which an individual receives access to the system.
Individual accounts come from BDN feed.

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?
None.

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.
No read-only accounts. Only accounts that can make changes to information.

WAVE – INTRANET (Admin site)
A potential user contacts the WAVE POC with justification for needing access. The POC establishes the account.

There are 2 user types:
1. Admin Accounts – Can establish RPO accounts, reset passwords for users and update email address
2. RPO Accounts – Can reset passwords for users and update email address

WAVE – INTERNET (Claimant site)
A potential user uses their Name, SSN, and VA File Number (if available) to log into the website. The website verifies said information against a BDN data import, containing the information of WAVE eligible users.

There is one user type:

2. User - Can view enrollment and eligibility data, verify enrollment, update Direct Deposit, update address information, view pending documents

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

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. The contractors are required to sign NDA's and Protection of Sensitive Information Agreements. 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, Information 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.

Contractors are bound by the same privacy and security procedures and requirements as VA employees.

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 Behavior (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 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 acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PII are required to complete privacy training annually.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* **Approved**
2. *The System Security Plan Status Date:* **18 May 2023**
3. *The Authorization Status:* **Authorization to Operate (ATO)**
4. *The Authorization Date:* **24 Apr 2023**
5. *The Authorization Termination Date:* **28 Jul 2023**
6. *The Risk Review Completion Date:* **24 Apr 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.***

Section 9 – Technology Usage

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

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

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

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

N/A

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

N/A

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.

N/A

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.

N/A

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).

N/A

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**

ID	Privacy Controls
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.

BERTHA BROWN Digitally signed by BERTHA BROWN
Date: 2023.08.31 12:41:09 -04'00'

Privacy Officer, Bertha Brown

Mark L. Ingold 187982 Digitally signed by Mark L. Ingold 187982
Date: 2023.08.30 08:32:32 -05'00'

Information System Security Officer, Mark Ingold

DARLA VAN NIEUKERK Digitally signed by DARLA VAN NIEUKERK
Date: 2023.09.06 09:39:50 -04'00'

Information System Owner, Darla van Nieukerk

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).

Veterans and/or beneficiaries applying for Education benefits must complete an application, VA Forms: 22-1990, 22-1990e, 22-1990n, 22-1990t, 22-1999, 22-199b and 22-6553c. The aforementioned forms include the Privacy Act Notice in the section labelled "Request to Opt Out of Information Sharing with Education Institutions."

Privacy Act Notice: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or title 38, Code of Federal Regulations, section 1.576 for routine uses (e.g., VA sends educational forms or letters with a veteran's identifying information to the veteran's school or training establishment to (1) assist the veteran in the completion of claims forms or (2) for the VA to obtain further information as may be necessary from the school for the VA to properly process the veteran's education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, and published in the Federal Register. Your obligation to respond is required to obtain or retain education benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law enacted before January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine the maximum benefits under the law. While you do not have to respond, VA cannot process your claim for education assistance unless the information is furnished as required by existing law (38 U.S.C. 3471). The responses you submit are considered confidential (38 U.S.C. 5701). Any information provided by applicants, recipients, and others may be subject to verification through computer matching programs with other agencies.

HELPFUL LINKS:

Record Control Schedules:

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

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices